Elgar

RESEARCH HANDBOOK ON International Law and Cyberspace

Edited by **Nicholas Tsagourias** • **Russell Buchan**

RESEARCH HANDBOOKS IN INTERNATIONAL LAW

Published by
Edward Elgar Publishing Limited
The Lypiatts
15 Lansdown Road
Cheltenham
Glos GL50 2JA
UK

Edward Elgar Publishing, Inc.
William Pratt House
9 Dewey Court
Northampton
Massachusetts 01060
USA

A catalogue record for this book
is available from the British Library

Library of Congress Control Number: 2021947698

This book is available electronically in the Elgaronline
Law subject collection
http://dx.doi.org/10.4337/9781789904253

ISBN 978 1 78990 424 6 (cased)
ISBN 978 1 78990 425 3 (eBook)

Contents

Contributors

Kai Ambos is Chair of Criminal Law, Criminal Procedure, Comparative Law, International Criminal Law and Public International Law at the Faculty of Law, Georg August Universität Göttingen, Germany. He is also Acting Director for the 'Institute for Criminal Law and Justice', Director for the 'Centro de Estudios de Derecho Penal y Procesal Penal Latinoamericano' (CEDPAL), Judge at Kosovo Specialist Chambers (The Hague, Netherlands) and Advisor (*amicus curiae*) to the Colombian Special Jurisdiction for Peace.

Constantine Antonopoulos LL.B (Thrace), LL.M (Cantab), Ph.D (Nottingham) is Associate Professor of Public International Law, Faculty of Law, Democritus University of Thrace. He is a member of several academic societies: the American Society of International Law; the European Society of International Law; the International Law Association (member of the board of the Hellenic Branch); and the Hellenic Society of International Law and International Relations. He is also a member of the ILA's Committee on the Use of Force (2009–present). He is the author of three monographs; a cases and materials book on the settlement of disputes by the International Court of Justice; and co-editor of a textbook on international law. Constantine has also authored several articles and chapters in books.

Louise Arimatsu is Distinguished Policy Fellow with the Centre for Women, Peace and Security at the London School of Economics and Principal Visiting Research Fellow with the School of Law, University of Reading. She was a member of the International Group of Experts to the Tallinn Manual on the International Law Applicable to Cyber Warfare (2013) and Legal Peer Reviewer to the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017).

Karine Bannelier is Associate Professor in International Law at the University Grenoble Alpes (France). She is Deputy Director of the Grenoble Alpes Cybersecurity Institute and of the Chair Legal and Regulatory Implications of Artificial Intelligence. Her main areas of interest are international security, the law of armed conflicts and the use of Force. Her research focuses on the capacity of international law to adapt to new challenges of international security in particular in cyberspace.

Giacomo Biggio Ph.D is a Teaching Associate at the University of Bristol. His research interests lie in the relationship between international humanitarian law and cyber-warfare, cyber-weapons and cyber-peacekeeping.

Eric De Brabandere is Professor of International Dispute Settlement Law and Director of the Grotius Centre for International Legal Studies. He is also Attorney-at-Law at the Brussels Bar (with DMDB Law) practicing in international law and investment arbitration, Editor-in-Chief of the *Leiden Journal of International Law*, and a member of the Board of Editors of the *Journal of World Investment & Trade*, the *Revue Belge de Droit International* (*Belgian Review of International Law*) and the Martinus Nijhoff Investment Law Book Series.

Russell Buchan is Senior Lecturer in International Law at the University of Sheffield, UK. Dr Buchan is the author of *International Law and the Construction of the Liberal Peace* (Hart, 2013) and *Cyber Espionage in International Law* (Hart, 2018) and he has authored many journal articles on the topic of international law.

Brigadier-General Prof. Dr **Paul A. L. Ducheine** MSc LL.M. is a Legal Advisor (Army Legal Service), and currently the Professor for Cyber Operations and Cyber Security at the Netherlands Defence Academy and a Professor of the Law of Military Cyber Operations at the University of Amsterdam. He obtained his Ph.D. on the legal framework for military counter terrorism operations in 2008, from the University of Amsterdam.

David P. Fidler is a Senior Fellow for cybersecurity and global health at the Council on Foreign Relations, USA.

Carlo Focarelli is Professor of International Law at Roma Tre Univesity, Rome. His works include: *International Law as Social Construct: The Struggle for Global Justice* (Oxford University Press, 2012); *The Law and Practice of the United Nations* (Brill/Nijhoff, 2016, 5th edn, with Benedetto Conforti), *International Law* (Edward Elgar, 2019).

Terry D. Gill: BA 1982, LLM 1985, PhD (*cum laude)* 1989, is Professor Emeritus of Military Law at the University of Amsterdam. He also held the chair of Military Law at the Netherlands Defence Academy. Prior to that he was first Assistant and later Associate Professor of Public International Law at Utrecht University. Professor Gill is editor in chief of the *Yearbook of International Humanitarian Law* and a member of the editorial board of various other journals. He was a member of the group of experts which drafted the 'Manual on International Law Applicable to Cyber Warfare' (also known as 'The Tallinn Manual'), drafted with support of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) between 2010–2013, and again for the second edition covering peacetime cyber activities between 2016 and 2018. He is author of numerous publications on the use of force, humanitarian law and military operational law.

Kathleen Heath is a Lawyer at the Aboriginal Legal Service of Western Australia and a graduate of Sydney and Harvard law schools.

Christian Henderson is Professor of International Law and Deputy Head of the Sussex Law School at the University of Sussex, UK. His research interests are within international conflict and security law, specifically the law governing the use of force and international humanitarian law. He is the author of several books, most recently *The Use of Force and International Law* (Cambridge University Press, 2018). He is a member of the International Law Association's committee on the Use of Force and a member of the Advisory Council of the Institute for International Peace and Security Law (University of Cologne, Germany).

Steven Hill completed a six-year term in office as the chief legal counsel at NATO headquarters in Brussels in 2020. He led a team that provided legal advice on issues including cyber defence. He served on NATO's Cyber Defence Management Board and the group of experts that drafted the Tallinn Manual 2.0. Prior to joining NATO in February 2014, Steve was Counsellor for Legal Affairs at the United States Mission to the United. From 2008 to 2010, he led the legal unit at the International Civilian Office / European Union Special Representative in Kosovo. He began practicing international law in the Office of the Legal Adviser at the

U.S. Department of State in 2001. He is a member of the Executive Council of the American Society of International Law and Associate Senior Policy Fellow at the Institute of Security and Global Affairs at Leiden University in the Netherlands.

Zhixiong Huang is the Changjiang Outstanding Young Scholar Professor and Vice Dean at the Law School as well as Executive Director of the Institute for Cyber Governance, Wuhan University, China. He served (or serves), among others, as member of the International Group of Experts of the Tallinn 2.0 Project on International Law Applicable to Cyber Operations, and Special Rapporteur of the Working Group on International Law in Cyberspace, Asian African Legal Consultative Organization (AALCO). His research focuses on public international law, especially international law in cyberspace.

Philipp Kastner is a Senior Lecturer at the Law School of the University of Western Australia. He holds degrees from McGill University, Canada (D.C.L. and LL.M.) and the University of Innsbruck, Austria (Dr. iur. and Mag. iur). He researches and teaches in the areas of the resolution of armed conflicts and transitional justice, international criminal law, public international law and legal pluralism. Publications include *Legal Normativity in the Resolution of Internal Armed Conflict* (Cambridge University Press, 2015) and *International Criminal Justice* in bello*?* (Martinus Nijhoff, 2012). He is also the editor of *International Criminal Law in Context* (Routledge, 2018) and co-editor of *The Politics of International Criminal Law* (Brill, 2021).

Ido Kilovaty is the Frederic Dorwart and Zedalis Family Fund Associate Professor of Law at the University of Tulsa, College of Law. Prior to Tulsa, Kilovaty was a Cyber Fellow at Yale Law School's Center for Global Legal Challenges and a Resident Fellow for the Information Society Project. Kilovaty studies the connection between technology, law and policy, with a focus on domestic and global cybersecurity. Kilovaty's most recent scholarship has appeared or is forthcoming in *UC Irvine Law Review*, *Ohio State Law Journal*, *Tennessee Law Review*, *Berkeley Technology Law Journal*, *Harvard National Security Journal* and the *North Carolina Journal of Law & Technology*.

Uta Kohl is Professor of Commercial Law at the University of Southampton, with an interest in corporate and internet governance. She has written widely on regulatory shifts triggered by the rise of global digital networks, and is author of *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (2007), co-author of *Information Technology Law* (2016); editor of *The Net and the Nation State* (2016) and co-editor of *Data-Driven Personalisation in Markets, Politics and Law* (2021).

Outi Korhonen is Professor of International Law (University of Turku). She is member of the Institute of Global Law and Policy (IGLP) at Harvard Law School and contributes to many academic publications as editor and author. Korhonen's research focuses on a wide variety of subjects including global governance, law and emerging technology, authority, methodology and critical approaches to international law. Korhonen has worked with both academia and government in Belgium, Egypt and the United States in addition to Finland.

Marja Lehto is Ambassador and Senior Expert in public international law at the Ministry for Foreign Affairs of Finland and Adjunct Professor of international law at the University of Helsinki, member of the UN International Law Commission and Special Rapporteur for the topic 'Protection of the Environment in Relation to Armed Conflicts'. Dr Lehto is also a member of the Council of the International Institute of Humanitarian Law and of the

Committee on Military Assistance on Request of the International Law Association. She has published on a broad range of international legal questions ranging from the law of the sea to State succession, peace and security, armed conflict and terrorism.

Ekaterina Markovich is doctoral candidate at the Faculty of Law in the University of Turku. She specialises in privacy and consent issues in the cyber-age. Markovich participates in international conferences and teaches a variety of international legal subjects. She has academic experience from Russia, Finland and Sweden.

Frédéric Mégret is a full-Professor and William Dawson Scholar at the Faculty of Law, McGill University and the co-Director of its Centre for Human Rights and Legal Pluralism. From 2006 to 2016 he held the Canada Research Chair on the Law of Human Rights and Legal Pluralism. Before coming to McGill, he was an assistant Professor at the University of Toronto, a research associate at the European University Institute, and an attaché at the International Committee of the Red Cross. He is the editor, with Philip Alston, of the forthcoming second edition of *The United Nations and Human Rights: A Critical Appraisal* and the co-editor of the *Oxford Handbook of International Criminal Law*. His research interests are in general international law, the laws of war, human rights and international criminal justice.

Eric Myjer is Emeritus Professor of Conflict and Security Law, School of Law, Utrecht University, the Netherlands. He is also associated with the research group on *The Role of Law in Armed Conflict and Military Operations* at the Amsterdam Centre for International Law, University of Amsterdam. He has published widely in the area of conflict and security law with a particular focus on arms control law as well as on deterrence theory. Professor Myjer is co-editor in chief of the *Journal of Conflict and Security Law* and serves as a locum Judge at the The Hague Court of Appeal.

Hitoshi Nasu is Professor of Law at the United States Military Academy, West Point. He is also a Senior Fellow at the Stockton Center for International Law, United States Naval War College, Newport. He publishes widely in the field of public international law, with particular focus on international security law and the law of armed conflict. His expertise extends to a wide range of international security law issues, such as collective security, peacekeeping, the protection of civilians in armed conflict, and in different domains including maritime, cyber and space.

Iñaki Navarrete is Associate Legal Officer and formerly Judicial Fellow at the International Court of Justice, The Hague. He is a graduate of the joint civil law and common law program of the Faculty of Law, McGill University. He has published on issues concerning general public international law, international human rights law, and intelligence collection in leading journals, including the *Canadian Yearbook of International Law* and the *Cornell International Law Journal*.

Colonel (GS) **Peter B. M. J. Pijpers** MSc LL.M is Associate Professor for Cyber Warfare at the War Studies Department at the Netherlands Defence Academy. His research, at the Amsterdam Center for International Law at the University of Amsterdam, focuses on transnational digital interference and intervention in political processes.

Marco Roscini is Professor of International Law at the University of Westminster. He holds a PhD from Sapienza University of Rome. Prof Roscini has published widely in the field of

International Conflict and Security Law. In particular, he is the author of *Le zone denuclearizzate* (Giappichelli, 2003), *Cyber Operations and the Use of Force in International Law* (Oxford University Press, 2014), and of many journal articles and book chapters. He is also the co-editor of *Non-proliferation Law as a Special Regime* (Cambridge University Press, 2012).

Neil C Rowe, Ph.D., is Professor of Computer Science at the Naval Postgraduate School where he has been since 1983. He has a Ph.D. in Computer Science from Stanford University and three other degrees from the Massachusetts Institute of Technology. His main research interests are artificial intelligence, processing of big data, the modeling of deception, information security, and digital forensics. He is the author of a book on artificial intelligence, a book on cyberdeception, and 220 refereed technical papers.

Ben Saul is Challis Chair of International Law at the University of Sydney, a counter-terrorism consultant for the United Nations, an Associate Fellow of the Royal Institute of International Affairs (Chatham House), and an Associate Fellow of the International Centre for Counter-Terrorism in The Hague.

Sergey Sayapin (LL.B., LL.M., Dr, iur., PhD) is an Associate Professor and Associate Dean at the School of Law, KIMEP University (Almaty, Kazakhstan). His current research focuses on Central Asian and post-Soviet approaches to international law, international and comparative criminal law, human rights, and sociology of law. He is the author of *The Crime of Aggression in International Criminal Law: Historical Development, Comparative Analysis and Present State* (T. M. C. Asser Press/Springer, 2014), co-editor of *The Use of Force against Ukraine and International Law: Jus Ad Bellum, Jus In Bello, Jus Post Bellum* (T. M. C. Asser Press/ Springer, 2018) and sub-editor for Central Asia of the *Encyclopedia of Public International Law in Asia* (Brill, forthcoming in 2021).

Michael N. Schmitt is Professor of International Law at the University of Reading, G. Norman Lieber Distinguished Scholar at the US Military Academy (West Point), Charles H. Stockton Distinguished Scholar-in-Residence at the US Naval War College, Strauss Center Distinguished Scholar and Visiting Professor of Law at the University of Texas, and Senior Fellow at the NATO Cooperative Cyber Defence Centre of Excellence. He has served as Director of the Tallinn Manual Projects since 2009.

Nicholas Tsagourias is Professor of International Law at the University of Sheffield. He has held visiting positions and research fellowships at Universities in France, Sweden and the United States. His teaching and research interests are in the fields of international law and the use of force, international humanitarian law, international criminal law, international constitutional law and cybersecurity. Professor Tsagourias has over 70 publications (books, articles and book chapters) on these issues. Among his publications are: *Regulating the Use of Force in International Law: Stability and Change* (Elgar, 2021 with Dr Russell Buchan); *Research Methods on International Law: A Handbook* (Elgar, 2021, with Dr Rossana Deplano); *International Humanitarian Law: Case, Materials, and Commentary* (CUP, 2018 with Lt Col Alasdair Morrison); *Collective Security: Theory, Law and Practice* (CUP, 2013 with Professor Nigel White). Professor Tsagourias sits on the editorial boards of the *Journal of Conflict and Security Law* and for the *Journal on the Use of Force and International Law*.

David Turns is Senior Lecturer in International Law at the Defence Academy of the United Kingdom (Cranfield University). He served for many years as the President of the

UK National Group of the International Society for Military Law and the Law of War, and sits on the Society's Board of Directors; he is also a member of the International Institute of Humanitarian Law (IIHL, Sanremo, Italy) and of the International Advisory Board of the *Hungarian Yearbook of International Law and European Law*. He has delivered academic papers at many conferences in the UK and internationally and has written over 60 peer-reviewed publications on various topics in public international law. He was a Visiting Professor at the University of Vienna and has lectured on international humanitarian and criminal law at the IIHL, the NATO School (Oberammergau, Germany), and the UK and Italian Staff Colleges, as well as being a co-founder of the Vienna Courses on International Law for Military Legal Advisers. He has also collaborated with the International Committee of the Red Cross, the Dutch Ministry of Defence and the Swiss Department of Foreign Affairs, as well as delivering legal components of UK Defence Engagement courses in countries around the world.

Ramses A. Wessel is Professor of European Law and Head of the Department of European and Economic Law at the University of Groningen, The Netherlands. His research expertise is in EU external relations law, EU foreign and security policy, international organizations and the relations between legal orders. He published widely on issues of European and international institutional law and participates in a number of international projects on the (legal) role of the European Union as a global actor. Ramses Wessel is Vice-President of the European Society of International Law (ESIL), and Member of the Governing Board of the Centre for the Law of EU External Relations (CLEER) in The Hague. He is Editor of a number of international journals in the field.

Yaohui Ying is a Ph.D. candidate at the Law School of Wuhan University. She holds a Bachelor of Law and a Master of Public International Law. Her research interests comprise international law in cyberspace and space law.

Preface

The first edition of this Handbook was published in 2015. Since then, cyberspace has penetrated all fields of human activity and this has opened up new opportunities but also brought about novel challenges. While States, institutions and the academy have intensified their efforts to better understand how international law applies to cyberspace and the activities occurring within it, there is still significant disagreement between them as to how international legal rules apply in practice.

A second edition of this Handbook is therefore necessary. This fully updated and expanded edition brings together a group of experts to examine in a knowledgeable and authoritative manner a host of legal issues pertaining to cyberspace and cyber activities. Chapters engage with current debates on how international law applies to cyberspace and they offer unique and insightful perspectives.

Part I of this Handbook examines the legal status of cyberspace and how certain international legal principles apply to it. These include rules on sovereignty, non-intervention, jurisdiction, State responsibility, human rights, individual criminal responsibility and international investment law and arbitration. Part I also contains chapters exploring norm development in cyberspace and how State and non-State actors exert power through this domain. Part II sets out and analyses the legal rules applicable to cyber terrorism, cyber espionage and cyber crime. Part III examines how the rules on the non-use of force and self-defence apply to cyber attacks. It also explores the notion of cyber operations, cyber deterrence and how international law applies to cyber-peacekeeping. Part IV considers the application of international humanitarian law to cyber war. In particular, it deals with ethical issues concerning cyber weapons, the classification of cyber conflicts, the principle of distinction, the notion of attack, the principles of proportionality and precaution and the law of neutrality. Part V examines international and regional approaches to cyber regulation and the application of international law to cyberspace as well as the cyber security policies of Russia, China, the EU, NATO, the Asia-Pacific nations and the United Nations.

This Handbook thus serves as a guide to academics, practitioners, researchers and students on the international law principles and rules that apply to cyberspace and cyber activities. It is an indispensable and rich source of knowledge that can also serve as a basis for further research in this area.

We are grateful to various people who have contributed in different ways to this Handbook. First, we are indebted to all the authors for their excellent contributions. Second, we are grateful to Professor Michael Schmitt for writing the introduction. Professor Schmitt has almost single-handedly placed cyber on the academic and policy agenda. Finally, we would like to thank Ben Booth, Laura Mann and the Edward Elgar team for facilitating the production of this Handbook.

Table of cases

INTERNATIONAL

International Centre for Settlement of Investment Disputes

World Trade Organization

EUROPEAN

European Court of Human Rights

European Court of Justice/Court of Justice of the European Union

NATIONAL

Australia

Belgium

Canada

France

Germany

Ireland

Israel

The Netherlands

United Kingdom

United States of America

Table of legislation

INTERNATIONAL LEGISLATION AND TREATIES

EUROPEAN UNION

NATIONAL

Australia

Canada

France

Germany

India

New Zealand

Russia

South Africa

The Netherlands

United Kingdom

United States of America

Introduction to the *Research Handbook on International Law and Cyberspace*

Michael N. Schmitt

Over the course of the last three decades, cyberspace has been 'woven into the fabric of daily life'[1] and now permeates all aspects of modern society: communication; information exchange and sharing; banking; shopping; conducting business; providing services; governing; law enforcement; national security and much more. Indeed, the Covid-19 pandemic laid bare the centrality of cyberspace by forcing many essential functions online. As of October 2020, 63.2 per cent of the world's population used the Internet (with usage in Europe being 87.2 per cent and in North America 90. 3 per cent), an increase of 1, 266 per cent since 2000.[2]

Notwithstanding the enormous benefits associated with cyberspace, it has also become a repository for various threats and vulnerabilities. Conventional threats and threat actors are metastasising to the cyber domain and cyberspace is also proving to have its own vulnerabilities, threat actors and threat vectors. They originate from governments, organised groups, businesses and individuals and their aims can be financial, criminal, military, political, intelligence related or purely malicious. Cyber threats can affect individuals, businesses and States and disrupt the maintenance of international peace and security without regard to physical, legal and political borders.

These realities render cyberspace a challenging environment for legal regulation. Although States and international organisations have on many occasions affirmed that international law applies to cyberspace,[3] how these rules apply in practice is often unsettled and, resultantly, subject to competing views. Invariably, questions about the efficacy of international law in regulating this domain and the activities occurring within it arise.

The first edition of this Handbook brought together leading international law scholars and practitioners to map out the international law principles, rules and regulatory frameworks that apply to cyberspace. They critically assessed how those principles, rules and frameworks apply to specific cyber activities and explored interpretative adjustments to enhance the regulatory potential of international law. Since the 2015 first edition, scholarly, institutional and State attention on cyber matters has increased. Notably, the publication of the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* in 2017 was a landmark achievement that made a significant contribution to clarifying the application of international

[1] 69th Session of the UN General Assembly A/69/112 (30 June 2014) 4, foreword by the UN Secretary-General, http://undocs.org/A/69/112.

[2] Internet World Stats: Usage and Population Statistics, https://www.internetworldstats.com/stats.htm. In Africa, usage is 41.7 per cent but it has grown by 13, 898 per cent since 2000.

[3] See, e.g, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security UN Doc A/68/98 (24 June 2013) and Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/70/174 (22 July 2015).

law to cyberspace. This being said, there is still a penumbra of indeterminacy surrounding the application of international law to cyberspace and cyber activities.

With this in mind, this updated and expanded edition of the Handbook builds upon the success of the first edition. Existing chapters have been revisited in order to take stock of legal, institutional and political developments since 2015, and new chapters have been added to examine novel topics, including the development of cyber norms, how power is exerted in and through the medium of cyberspace, cyber intervention, the application of international investment law and arbitration to cyberspace, cyber-peacekeeping and regional perspectives.

The second edition thus provides a broad account of the international law rules applicable to cyberspace and cyber activities; engages in a systematic, knowledgeable and authoritative analysis of how they apply; provides an assessment of their suitability and effectiveness; and, where international law is found lacking, offers suggestions for new interpretations or regulatory approaches. It offers a comprehensive examination of the subject that will be invaluable to the work of policy makers, lawyers, political scientists, the military, law enforcement officials, technologists, researchers, as well as to students. I heartily congratulate the individual authors and both editors for their efforts in bringing this important project to successful completion. It is a work that will continue to influence and shape this complex – but central – facet of international law.

OVERVIEW OF THE CHAPTERS

The first part of the Handbook comprises nine chapters that focus upon the application of general principles of international law to cyberspace. In the opening chapter, Nicholas Tsagourias examines the legal status of cyberspace under international law, challenging the position that States cannot exercise sovereignty in cyberspace. If sovereignty denotes power and authority, he argues, States may exercise sovereignty over persons, objects and actions in cyberspace. For him, sovereignty is a stand-alone principle that is legally consequential. He rejects the premises that cyberspace can itself be sovereign or that big tech companies can be sovereign. Finally, Tsagourias considers the question of whether cyberspace can be a global commons, concluding that its features do not support such a characterisation. Lastly, he ends his study by opining that a global treaty to regulate cyberspace is not on the agenda at this stage.

In Chapter 2 Marja Lehto charts the rise of cyber norms. Lehto first explores the meaning of the term 'norm'. In doing so, she distinguishes between non-binding and binding norms and assesses their contribution to standard setting within the international community. Next, Lehto examines the role of the UN Group of Governmental Experts in developing cyber norms. Finally, she considers how the activities of the Group of Governmental Experts have been received within the wider international community.

In Chapter 3 Outi Korhonen and Ekaterina Markovich examine power dynamics in cyberspace by mapping its terrain, actors and structures. They argue that cyberspace is intertwined with our 'real world' space. The algorithms and codes that structure the functions of cyberspace separate the valuable from the valueless but in doing so they can exacerbate societal inequalities and polarisation. The authors contend that by familiarising ourselves with the concepts, actors, structures, debates and even wars of cyberspace, we have a better chance to identify the levers of influence, and hinder misuse of power, within cyberspace. They do so by

situating such topics as surveillance, privacy, encryption, AI, blockchain and VPNs in context in order to locate interdependencies and power struggles.

In Chapter 4 Uta Kohl examines when States can exercise their jurisdiction in cyberspace and, in particular, when they can extend their jurisdiction over powerful tech platforms and co-opt them into the business of territorial regulation. It traces judicial and legislative jurisdictional developments in this area, set against customary international law on legislative, adjudicative and executive jurisdiction. This chapter posits that the authority of the territorial State is not weakened by the rise of a global network society and might even be strengthened by it.

In Chapter 5 Ido Kilovaty studies the international law of cyber intervention since, as he says, cyberspace has become a domain and a tool of interference. He contends that, although international law prohibits external intervention in the domestic and foreign affairs of another State, the way in which the prohibition applies to interference through cyberspace is often contested, particularly with respect to intervention's element of coercion. Indeed, he looks at ways in which emerging interference technologies and cyberspace challenge the basic tenets of non-intervention. Kilovaty maintains that expanding our understanding of coercion, informing its scope through human rights, and acknowledging the role of manipulation, disinformation and disruption is crucial for the future of non-intervention in cyberspace.

In Chapter 6 Constantine Antonopoulos suggests that although the rules relating to the responsibility of States for internationally wrongful acts apply to State conduct in cyberspace, such applicability is fraught with difficulties because this legal framework is premised upon the assumption that internationally wrongful acts are capable of attribution to States. As Antonopoulos explains, this is problematic in the context of cyberspace because of its unique characteristics, such as the anonymity that cyberspace affords. In light of this, he argues that the best solution is to subject States to a duty of due diligence to prevent computer systems that fall within their jurisdiction from being used to commit acts that are injurious to other States.

In Chapter 7 David Fidler addresses the relationship between cyberspace and human rights. For him, cyberspace challenges certain principles of international law central to the protection of human rights, such as the principle of sovereignty and jurisdiction. For instance, it raises questions as to whether Internet access is a human right and how the concept of, and debate over, the extraterritoriality of human rights law applies in the cyber context. The cyberspace-human rights relationship also evokes questions as to national and international policies on Internet governance and cyber security, an important issue given Edward Snowden's revelations concerning the United States National Security Agency's massive cyber surveillance campaign. Fidler concludes by noting that cyberspace is subject to international politics that have historically affected human rights protection, with examples including the resilience of sovereignty, national security concerns and shifting balances of power. As a result, he suggests that cyberspace's potential to significantly enhance the enjoyment of fundamental human rights may be never fully realised.

In Chapter 8 Kai Ambos considers whether the commission of hostile cyber operations can give rise to individual criminal responsibility, with particular reference to the provisions of the Rome Statute. Ambos examines the conditions by which individuals may be held criminally responsible for war crimes and crimes against humanity and applies them in the cyber context. He also asks whether cyber aggression can fall within the definition of the crime of aggression under the Rome Statute and whether criminal jurisdiction can be exercised over cyber aggression.

In Chapter 9 Eric De Brabandere explores the possible connections between international investment law and arbitration on the one hand and foreign investment in cyberspace on the other. He examines whether digital assets can qualify as 'investments' as well as the related question of entry requirements for foreign investors and security screening operated by host States for investments in digital assets. He also assesses possible claims by foreign investors against host States for breaches of their obligations under applicable international investment treaties in relation to cybersecurity.

Part II of the Handbook assesses the extent to which international law adequately deters and suppresses threats that emerge in and from cyberspace. In Chapter 10 Ben Saul and Kathleen Heath evaluate whether international terrorism conventions apply to cyber terrorism. Although they conclude that certain terrorism conventions can be interpreted in such a manner, they assert that gaps remain in legal regulation, not the least of which is that there is no definition of terrorism (and, for that matter, of cyber terrorism). They query whether cyber terrorism would be better addressed through the negotiation and conclusion of a direct and specific international treaty.

In Chapter 11 Russell Buchan and Iñaki Navarrete examine the impact of political and economic cyber espionage on the maintenance of international peace and security, determining that such practices can have a destabilising effect upon international cooperation and the stability of the international economic order. They then consider how international law applies to political and economic cyber espionage, including an assessment of the principle of territorial sovereignty and the law of the World Trade Organization.

Chapter 12 focuses upon cyber crime and the role of national, regional and international law in combating this activity. Philipp Kastner and Frédéric Mégret argue that many crimes committed in cyberspace are regulated by domestic criminal legal systems. They illustrate this by reference to specific crimes committed in cyberspace. The application of domestic criminal law notwithstanding, Kastner and Mégret suggest that in order to achieve adequate criminal law enforcement, multilateral initiatives such as the Council of Europe's Convention on Cybercrime are essential, for they lay the foundations for greater cooperation between States. Indeed, Kastner and Mégret conclude that a multilateral treaty to mandate global cooperation beyond State or regional boundaries, and across the State/non-State divide, is needed to deal with many forms of cyber crime

Part III examines the relationship between hostile cyber operations and the *jus ad bellum*. To provide background, Paul Ducheine and Peter Pijpers explore the notion of cyber operations in Chapter 13. They argue that, at the State level, there are broadly five distinct paradigms that can be used to describe cyber operations: governance; protection; law enforcement; intelligence; and military operations. The authors assert that it is the last paradigm that constitutes the most far-reaching framework for governmental action and suggest that the proliferation of concepts such as cyber attacks, cyber targeting and cyber war are indicative of the growing militarisation of cyberspace.

Chapter 14 considers whether hostile cyber operations constitute unlawful uses of force under Article 2(4) UN Charter. Marco Roscini argues that force within the meaning of Article 2(4) requires the use of a weapon accompanied by a coercive intention and effects. He explains that, in the cyber context, this occurs when an operation against a computer system results in physical damage to property or loss of life or injury to people. He also advocates a reading of Article 2(4) that extends to cyber operations which, while not manifesting real-world damage,

nevertheless render ineffective or unusable computer systems that sustain critical infrastructures and thus cause significant disruption to the delivery of essential services.

Following on from this assessment of Article 2(4), in Chapter 15 Carlo Focarelli examines the circumstances by which a cyber operation can amount to an armed attack pursuant to Article 51 UN Charter and thus trigger a State's right to use force in self-defence. In particular, and with reference to State practice and recent literature, Focarelli debates whether an armed attack can be said to occur only where the cyber operation produces sufficiently serious physical damage or instead whether its application extends to sufficiently serious non-physical damage. A cyber operation that affects the functionality of computer systems sustaining critical national infrastructure illustrates the latter. In addition, Focarelli considers how the principles of necessity and proportionality apply to cyber uses of force that are committed in accordance with Article 51 UN Charter.

In Chapter 16 Nicholas Tsagourias and Giacomo Biggio discuss how international law applies to cyber-peacekeeping. They first explain which peacekeeping tasks can be 'cyberized' and then discuss the technical and legal challenges that arise with regard to the peacekeeping principles of consent, impartiality and use of force in self-defence. Tsagourias and Biggio go on to examine the regulation of the use of lethal force by cyber peacekeepers in and outside situations of armed conflict. In what is the first comprehensive legal study of cyber-peacekeeping, they identify institutional, political and legal challenges affecting cyber-peacekeeping and make recommendations to address them.

States might seek to protect their cyber infrastructure against military cyber threats by recourse to the language of deterrence, that is, by asserting that they will respond to cyber operations with a devastating cyber operation of their own. In Chapter 17 Eric Myjer compares deterrent strategies in the nuclear realm with deterrence in the cyber arena. He argues that because of the unique features of cyberspace, cyber deterrence is not comparable to nuclear deterrence. Therefore, in his estimation, cyber deterrence is unlikely to prove effective. Myjer concludes by arguing that deterrence by the threat of cyber retaliation would be contrary to certain basic principles of international law, such as necessity and proportionality.

Part IV focuses on the use of cyber technology during times of armed conflict and in particular on the application of international humanitarian law to cyber weapons and to hostilities conducted in cyberspace. In Chapter 18 Neil Rowe identifies various important ethical concerns unique to the use of cyber weapons. These include attribution, product tampering, unreliability, damage repair and collateral damage. He concludes that many of these concerns are intractable. As a result, he encourages the development of international treaties to restrict and regulate their use.

In Chapter 19 Louise Arimatsu addresses how cyber conflicts can be classified under international humanitarian law and, most notably, whether cyber conflicts give rise to an international or a non-international armed conflict. This inquiry involves consideration of whether cyber operations satisfy the requirement of 'international', 'armed' and 'attack' for the purpose of international armed conflict. In relation to non-international armed conflict, the key questions are whether cyber groups can be regarded as 'organised' and whether cyber conflict can be ever of sufficient intensity to trigger the application of international humanitarian law.

In Chapter 20 Karine Bannelier assesses whether the principle of distinction is still relevant to hostilities conducted in cyberspace. Bannelier explains that the principle of distinction applies only to conduct that amounts to an attack under international humanitarian law, which conventionally requires the use of violence that produces physical damage. Bannelier criticises

this conclusion given that in the contemporary era States place heavy reliance on cyberspace and thus conduct that affects the functionality of computer systems can be extremely damaging even if it does not cause physical damage. As a result, she argues that a better approach is to subject all military operations (including those in cyberspace) to the principle of distinction regardless of the damage they cause. Customary international law, at least according to Bannelier, supports such an approach. She also stresses the difficulty of distinguishing between military and civilian objects in cyberspace given its inherent interconnectivity and also explores how the concept of direct participation in hostilities applies to individuals involved in devising, maintaining and implementing cyber operations during times of armed conflict.

Chapter 21 examines the application of the principle of proportionality and the duty to take precautions in attack to operations carried out in the cyber domain. Terry Gill argues that a cyber operation would only qualify as an 'attack' for the purpose of international humanitarian law if it is committed in the context of a recognised armed conflict and is intended to, or reasonably likely to cause, appreciable danger of physical harm or damage. He concludes that while many cyber operations would therefore not qualify as attacks, some would and, for those, international humanitarian law would be applicable by analogy in much the same way as it applies to attacks by kinetic weapons. Thus, cyber operations against purely military installations or combatants, without any likely appreciable consequences to civilians or civilian objects, would fall outside the applicability of proportionality. Cyber operations directed against military objectives or combatants that incidentally harm civilian objects or civilians are subject to the proportionality test and would be unlawful if the expected damage to the civilian objects or civilians is likely to be excessive in relation to the anticipated military advantage.

In Chapter 22 David Turns assesses the application of the law of neutrality to cyberspace. Turns explains that this is a complicated process because the law of neutrality was devised more than a century ago and was therefore constructed with the intention of protecting the territorial sovereignty of neutral States, namely, tangible constructs such as physical territory, territorial waters and territorial airspace. By contrast, cyberspace is an intangible and interconnected environment. This considerably enhances the potential for operations in cyberspace to implicate third parties. Turns concludes that the law of neutrality is still relevant to cyberspace by analogy and proceeds to examine how neutrality affects the conduct of cyber operations by neutrals and belligerents.

Part V reviews the approaches of various international organisations to regulating activities in cyberspace and, in particular, to achieving and maintaining cyber security. In Chapter 23 Ramses Wessel explains that over the past decade the EU has started to take its first steps in formulating and regulating cyberspace as a new policy area, especially since the adoption of its 2013 Cyber Security Strategy. In an exploratory fashion, Wessel's chapter evaluates both the EU's existing and emerging internal cyber security rules, as well as the EU's contribution to the development of a global regulatory framework for cyberspace.

In Chapter 24 Steven Hill examines NATO's strategy for achieving cyber security. The chapter has three core objectives. First, it describes the cyber threat environment as perceived by NATO. Second, it provides a historical overview of the evolution of NATO's cyber policy and the development of NATO structures. Third, it highlights some of the international law issues faced by NATO in recent years and explores how the international community more broadly may draw upon and learn from these experiences.

In Chapter 25 Sergey Sayapin examines Russia's approach to international law in cyberspace. He argues that Russia appears to stray some distance from international law-making efforts in order to reinforce its own information security through domestic legislation. He then analyses a number of domestic legal acts regulating activities in cyberspace that do not generally refer to international law, except those relating to the use of force. Finally, Sayapin predicts that Russia's relatively isolationist stance is likely to continue in the foreseeable future.

In Chapter 26 Zhixiong Huang and Yaohui Ying present China's agenda for international cyberspace governance and rule-making. For them, it is informed by the idea of 'a community with a shared future in cyberspace' and the 'multilateral plus multi-party' pluralism of cyberspace governance model. Aspiring to shift from a 'norm-taker' to a 'norm-maker', China has formed its own position on international law in cyberspace. According to the authors, China combines the application of existing international law with setting new soft law and formulating new hard law under UN apparatus. Huang and Ying also explain China's support for the principle of sovereignty in cyberspace, which can be contrasted with its approach to the *jus ad bellum* and the law of armed conflict. They conclude by suggesting that, notwithstanding China's belief in a rule-based system for cyberspace and its norm entrepreneurism, China will have to face up to a number of legal and political challenges.

Hitoshi Nasu explores Asia's approach to achieving cyber security in Chapter 27. Nasu notes that cyber security has become a key priority for many Asia-Pacific States, although he opines that achieving cyber security in this region is likely to be a complex and difficult task because of its political, economic and socio-cultural diversity. He identifies cyber security policy initiatives adopted by institutions in the Asia-Pacific region, such as ASEAN and APEC. Nasu maintains that regional cyber security efforts have been somewhat frustrated by the traditional security challenges that confront many States in the region.

In Chapter 28 Christian Henderson reviews the role and activities of the UN in the cyber security context. He argues that while the UN has historically been sluggish in taking on cyber security issues, it has, in the wake of the dramatic increase in cyber operations since 2007, gradually begun to address this topic. In particular, activity can be seen in various committees of the UN General Assembly, including the achievement of consensus within several Groups of Governmental Experts on various cyber issues. Additionally, issues of cyber security have surfaced in the UN Security Council, the Economic and Social Council and other subsidiary organs and specialised agencies. Henderson welcomes the decision of these UN agencies to address cyber security, but explains that their next challenge is to cooperate more closely in order to ensure an integrated and concerted response to the maintenance of cyber security.

CONCLUSION

Although it is by now fairly well settled that international law applies to activities in cyberspace, the jury is still out on how to apply such law. This Handbook engages that dialogue in a sophisticated and insightful manner. I admit to disagreeing with some of the reasoning and conclusions reached by individual contributors. Nevertheless, even in such cases, I find the analysis highly incisive and intellectually provocative. I again congratulate my friends Nicholas Tsagourias and Russell Buchan on bringing together such a talented group to so usefully examine one of the most complex topics being grappled with by the international law community.

1. The legal status of cyberspace: sovereignty redux?

Nicholas Tsagourias

1. INTRODUCTION

Cyberspace is sometimes described as a purely non-legal domain. According to John Barlow's *A Declaration of the Independence of Cyberspace* 'legal concepts do not apply to cyberspace'.[1] The view of cyberspace as a non-legal domain is based on a number of assumptions. The first assumption is that cyberspace is different from real spaces: its a-territorial, borderless and ubiquitous character differentiates it from the physical and bounded spaces that are subject to legal regulation. The second assumption is that cyberspace, true to its original conceptualisation and design and the involvement of multiple stakeholders, should remain an open, decentralised and participatory space not hampered by legal regulation or, at least, not subjected exclusively to State-led regulation.[2]

Yet, the view that cyberspace is subject to law and indeed to international law is not in dispute anymore. The 2013 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security [GGE] affirmed that international law and in particular the United Nations [UN] Charter as well as State sovereignty and the international norms and principles that flow from sovereignty apply to cyberspace.[3] As the UN Secretary-General also noted in the foreword to the report, '[t]he recommendations point the way forward for anchoring ICT security in the existing framework of international law and understandings that govern State relations and provide the foundation for international peace and security'.[4] The 2015 GGE Report went even further by setting out specific international norms and principles that apply or should apply to cyberspace. The Report lists 11 'voluntary, non-binding norms, rules or principles of responsible behaviour of States' to promote an open, secure, stable, accessible and peaceful cyber environment.[5] It also lists six international law principles that apply to cyber space and cyber activities, one of which is the principle of sovereignty as also reaffirmed

[1] John P Barlow, 'A Declaration of the Independence of Cyberspace' (Davos 1996) https://www.eff.org/cyberspace-independence.

[2] David R Johnson and David G Post, 'Law and borders: The rise of law in cyberspace' (1996) 48 *Stanford Law Review* 1367. *Contra* see Jack L Goldsmith, 'Against cyberanarchy' (1998) 65 *University of Chicago Law Review* 1199.

[3] UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc A/68/98 (24 June 2013) paras 19–20.

[4] Ibid., 4.

[5] UNGA, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc A/70/174 (22 July 2015) para 13.

in the 2021 GGE Report.[6] Various States or international organisations have also affirmed the application of international law to cyberspace.[7]

Applying international law to cyberspace is important for many reasons. The first reason is that international law performs a regulatory function by setting out the principles and rules that apply to cyberspace thus shaping conduct and determining what is legal and what is illegal. Second, it plays a performative function by constructing in legal terms the ontology, identity, and status of cyberspace. Third, international law embeds in its principles and rules authoritative choices about the nature, content, and use of cyberspace whilst at the same time moulds such choices through its own principles and rules. In doing so, international law 'naturalises' cyberspace because it embeds it into known legal categories and models of regulation and promotes stability and order not only in cyberspace but also in the international environment to which cyberspace is an appendix.

This chapter will thus examine the legal status of cyberspace as well as the status and import of the principle of sovereignty in cyberspace. The chapter is structured as follows. Section 2 discusses the nature of cyberspace and argues that cyberspace combines a physical, a social and a logical layer. Section 3 explores the question of whether the principle of sovereignty applies to cyberspace. In order to do this, the chapter explains the place, role and content of the principle sovereignty in international law and concludes that cyberspace is subject to the principle of sovereignty. Section 4 considers the legal status and import of the principle of sovereignty in cyberspace in view of claims that deny its legal significance in cyberspace. It contends that the principle of sovereignty is a legal principle that produces legal consequences. Section 5 explores the question of whether cyberspace itself can become sovereign but con-

---

[6] Ibid., para 26. 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security', UN Doc A/76/135 (14 July 2021) para 71(b).

[7] Finland, *International law and cyberspace: Finland's national position* (2020) 1–3, https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859; *Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace* (July 2020) https://www.aldiplomasy.com/en/?p=20901; Kersti Kaljulaid, President of Estonia, *President of the Republic at the opening of CyCon 2019* (29 May 2019) https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html; République Française, Ministère des Armées, *Droit International Appliqué aux Opérations dans le Cyberespace* (2019); The Netherlands, *Letter to the parliament on the international legal order in cyberspace* (5 July 2019) https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace; Portugal, *National Strategy for Cyberspace Security 2019-2023* Portuguese Official Journal, Series 1 - No. 108 - 5 June, 2019, Annex, section 1; UK United Kingdom Attorney General's Office, *Cyber and International Law in the 21st Century* (23 May 2018) https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century; Australia, *Australia's International Cyber Engagement Strategy* (4 October 2017) Annex A: Australia's position on how international law applies to state conduct in cyberspace, available at https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/australias-international-cyber-engagement-strategy; Brian Egan, 'International Law and stability in cyberspace' (2017) 35 *Berkeley Journal of International Law* 169; Harold Hongju Koh, 'International law in cyberspace' (2012) 54 *Harvard Journal of International Law Online* 1. For the views of OAS member States see OEA/Ser.Q, CJI/doc. 603/20 rev.1, 5 March 2020, 18–20 and OEA/Ser.Q, CJI/doc. 615/20 rev.1, 7 August 2020, 28–32. For China's views on sovereignty see Huang and Ying (Ch 26 of this Handbook). For NATO, see Wales Summit Declaration, 5 September 2014 para 62, available at: https://www.nato.int/cps/en/natohq/official_texts_112964.htm and Hill (Ch 24 of this Handbook).

cludes that this is impossible because it is intermediated by States and their people. It also contends that big tech companies that control cyberspace and its infrastructure are not sovereigns. Section 6 discusses but rejects the proposition that cyberspace can become a global commons because it does not fulfil the requisite criteria and because States have expressed no desire to designate it as such. Section 7 contains concluding remarks.

2. WHAT IS CYBERSPACE?

Questions as to what cyberspace is, and more specifically whether cyberspace is a corporeal entity, an intangible entity or a bundle of functions have technical, philosophical, political, sociological, and legal origins and ramifications.[8] Although I will not engage here with the various debates concerning the ontology of cyberspace for lack of expertise, I will offer a description of cyberspace in order to grasp the object of the enquiry because its features and attributes shape the way international law understands and, consequently, treats cyberspace. International law can then apply its principles and rules to cyberspace on the basis of legal assumptions, analogies, and categorisations or develop purpose-built legal principles and rules.

According to Kuehl's definition, cyberspace is 'a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies'.[9] According to another definition, cyberspace is composed of three layers: a physical layer composed of the cyber infrastructure; a second layer of software logic; and, a third layer of data.[10] These definitions highlight the physical and informational dimensions of cyberspace but omit the human dimension of cyberspace. In my opinion, the most inclusive definition and the one adopted for the purposes of this chapter is the definition provided by the US Department of Defense which identifies three co-joint components of cyberspace. As it explains 'cyberspace can be described in terms of three interrelated layers: physical network, logical network, and cyber-persona'.[11] The physical layer consists of the IT devices and infrastructure such as computers, integrated circuits, cables, communications infrastructure, servers, routers, switches; the logical layer consists of the software logic, data packets and electronics; and the cyber-persona layer consists of 'digital representations of an actor or entity identity in cyberspace'.[12] Cyber-personas may relate to real people but may also be artificial whereas a person may have multiple digital personas. This layer can alternatively be described

---

[8] David Koepsell, *The Ontology of Cyberspace: Law, Philosophy, and the Future of Intellectual Property* (Open Court Publishing 2003) 10; Julie E Cohen, 'Cyberspace as/and space' (2007) 107 *Columbia Law Review* 210.

[9] Daniel T Kuehl, 'From cyberspace to cyberpower: Defining the problem' in Franklin D Kramer, Stuart H Starr and Larry K Wentz, *Cyberpower and National Security* (National Defense University Press 2009) 28.

[10] Lior Tobanksy, 'Basic concepts in cyber warfare' (2011) 3 *Military and Strategic Affairs* 75, 77–8.

[11] US Department of Defense, *Cyberspace Operations*, Joint Publication 3-12 (8 June 2018) I-2. See also AJP–3.20, Allied Joint Doctrine For Cyberspace Operations, Edition A Version 1 (January 2020) 1.9–1.12.

[12] US Department of Defense, *Cyberspace Operations*, Joint Publication 3-12 (8 June 2018) I–4.

as the social layer of cyberspace and this is how it will be referred to in the remainder of this chapter. These layers are not separate but intertwined. Even if the core of cyberspace is virtual and cyber interactions are conducted through logistics rather than through physical acts, they are dependent on the physical and social layer of cyberspace.

Understanding the nature of cyberspace is also important because different disciplines may focus on different layers; for example, computer science usually focuses on the logical layer whereas law, and international law for that matter, focuses on the physical and social layer of cyberspace to the extent that law governs objects, persons, spaces, relations, or effects.

Having explained the nature of cyberspace and having identified its layers, in the next section I will examine the application of the principle of sovereignty to cyberspace because sovereignty is a foundational principle of international law.

3. CYBERSPACE AND SOVEREIGNTY

In its traditional definition, sovereignty denotes *summa potestas* that is, supreme and plenary authority and power.[13] According to Bodin who introduced the concept of sovereignty in political theory, sovereignty is an organising principle representing the consolidation and indivisibility of power within a political entity.[14] Bodin identified the holder of such power in the person or institution of the sovereign and, in doing so, he subjectivised sovereignty.

Sovereignty is also a foundational principle of international law. As the International Court of Justice (ICJ) said in the *Nicaragua Case,* the whole international law rest upon sovereignty.[15] Sovereignty is constitutive of international law because it gives international law its ontology; it is an organising principle in that it identifies the units of authority in international law and international relations and defines and delimits their competences and powers; it is an operational principle because it is the engine that generates, applies, and enforces international law; and it is functional principle because it determines whether and to whom international law applies.

In international law, the holder of sovereignty is the State. As a State attribute, sovereignty is a unitary concept joining together its internal aspect of supreme, plenary and exclusive authority and power within the State[16] and its external aspect of autonomy and independence vis-à-vis other States, plenary power to regulate externalities, and power to create, implement, and enforce international law. In the words of Judge Alvarez, by sovereignty 'we understand

---

[13] Alan James, *Sovereign Statehood* (Allen & Unwin 1986) 267–9; Francis Harry Hinsley, *Sovereignty* (CUP 1986); Stephen D Krasner, *Sovereignty: Organized Hypocrisy* (Princeton University Press 1999) 1–42; Samantha Besson, 'Sovereignty' in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (OUP 2012).

[14] Jean Bodin, *Les six livres de la Republique*, 1576, livre I, ch. 8, 131.

[15] *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)*, Judgment (Merits) [1986] ICJ Rep 14, para 263.

[16] As was said in *The Exchange v McFaddon*, 11 U.S. (7 Cranch 116) 116 (1812):
> The jurisdiction of a nation within its own territory, is exclusive and absolute. It is susceptible of no limitation not imposed by itself. Any restriction deriving validity from an external source would imply a diminution of its sovereignty to the extent of that restriction, and an investment of that sovereignty to the same extent in that power which could impose such restriction.

the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other States, and also in its relations with other States'.[17]

That having been said, it is true that sovereignty in international law has a strong territorial dimension.[18] This can be explained by the fact that its emergence as a political and legal concept coincided with the emergence of the State as a political unit following the apportionment of territories and the political and legal recognition of such territorial compartmentalisation by the Treaty of Westphalia.[19] The Peace of Westphalia redrew the political boundaries of authority from the previous state of overlapping authorities within the same territory to that of consolidated, supreme and plenary authority over a distinct piece of territory which was curved out because of the successful assertion of power by a single authority, the sovereign.

It follows from this that territory is not just a geographical or physical construct but a legal and political construct: it concerns the organisation of spaces for political and legal purposes or, put differently, it refers to a mode of organising sovereign power.[20] Territory provides a bounded and defined space where sovereignty can manifest itself exclusively and be realised effectively; it draws internal as well as external physical, legal and political borders without which sovereignty would remain abstract and unsubstantiated; it organises sovereignties and provides order in the international society by allowing States to coexist side by side without encroaching onto another's sovereignty. However, even if territory is an aspect of sovereignty and is protected by sovereignty, it is not synonymous with sovereignty. It is a container of sovereignty but sovereignty as authority and power can extend beyond territory. In other words, sovereignty is both territorial and a-territorial. In the latter case, the expanse of sovereignty and any limitations thereto are subject to sovereignty itself and not to territory.[21] It is for this reason that in this chapter I use the term 'principle of sovereignty' or 'State sovereignty' rather than 'territorial sovereignty'.[22]

Having explained the meaning of sovereignty in international law and its relation to territory, the question to ask is whether the principle of sovereignty can apply to cyberspace. Barlow's *Declaration of the Independence of Cyberspace* envisioned cyberspace as a space not subject to sovereignty. In academic writings, Johnson and Post argued that cyberspace cannot be subject to sovereignty but instead, cyberspace should be subject to its own distinct system of

---

[17] *Corfu Chanel Case* (*UK v Albania*) (Separate Opinion of by Judge Alvarez) [1949] ICJ Rep 43.

[18] Jens Bartelson, *A Geneology of Sovereignty* (CUP 1993) 26. See also Montevideo Convention on the Rights and Duties of States (signed 26 December 1933, entered into force 26 December 1934).

[19] Peace of Westphalia, signed on 30 January 1648 and 24 October 1648. The Peace of Westphalia and its contribution to international law is one of the foundational 'myths' of international law notwithstanding any contrary views. See Daniel Bethlehem, 'The end of geography: The changing nature of the international system and the challenge to international law' (2014) 25 *European Journal of International law* 9, 13; Nicholas G Onuf, 'Sovereignty: Outline of a conceptual history' (1991) 16 *Alternatives: Global, Local, Political* 425, 437.

[20] Thomas Forsberg, 'Beyond sovereignty, within territoriality: Mapping the space of late-modern (geo) politics' (1996) 31 *Cooperation and Conflict* 355; John G Ruggie, 'Territoriality and beyond: Problematising modernity in international relations' (1993) 47 *International Organization* 139. As Judge Max Huber opined, 'territorial sovereignty serves to divide between nations the space upon which human activities are employed'; *Island of Palmas Case (or Miangas)* (*United States v Netherlands*) [1928] Reports of International Arbitral Awards 839.

[21] Richard T Ford, 'A history of jurisdiction' (1999) 97 *Michigan Law Review* 843, 853–4.

[22] Peter J Taylor, 'The state as container: Territoriality in the modern world-system' (1994) 18 *Progress in Human Geography* 151.

legal regulation.[23] For them, it is not only the borderless and a-territorial nature of cyberspace that make it adverse to the standard system of territorially-based international legal regulation based on the overlap between the physical space represented by States and the 'law-space', but also the fact that sovereignty's principles of validity exhibited in territorially-based entities in the form of power, legitimacy, effects and notice are impossible or at best diluted in cyber-space. More specifically, the lack of borders in cyberspace deprives sovereigns of the ability to exercise their power over defined peoples and territories and deprives sovereign power from the legitimising effect of consent. It also deprives users from notice when entering a different jurisdiction. It is because of these features and the need to have an effective regulatory system appropriate to cyberspace that cyberspace should develop its own regulatory system based on self-regulation.[24]

The no-sovereignty thesis described above is based on a concept of cyber-exceptionalism and on a territorial reading of sovereignty. It should be noted however that Johnson and Post do not deny that law has a role to play in cyberspace but they propose a different regulatory system which is more appropriate to the features of cyberspace.

The normative premises of the no-sovereignty thesis were challenged by Jack Goldsmith in his article 'Against cyberanarchy'. [25] For him, there is nothing unexceptional as far as cyberspace is concerned whereas the jurisdictional and enforcement inadequacies of sovereign power in cyberspace identified by Johnson and Post have been exaggerated. As he explains, cyberspace consists of persons and objects and for this reason States can exercise power over people and objects on their territory. States can also regulate the local effects of extraterritorial activities. Also, traditional legal tools can resolve the multi-jurisdictional problems implicated in cyberspace and thus overcome the problem of legitimacy and validity. Furthermore, the standard rules of enforcement based on a person's location, personal jurisdiction or extradition can also apply to cyber activities. Regarding the issue of notice, Goldsmith says that there is a general notice that data may cross frontiers. In sum, according to Goldsmith, territorial sovereigns can regulate cyberspace through existing techniques.

From the preceding discussion it transpires that whether sovereignty applies to cyberspace boils down to the question of whether a State can exercise jurisdiction over cyberspace or, more specifically, over its layers. The reason that jurisdiction emerges as the defining attribute is because jurisdiction is the instantiation of the legal dimension of sovereignty in the form of prescription, application, enforcement, and adjudication.[26]

In cyberspace, a State can assert its sovereignty by exercising jurisdiction over the cyber infrastructure located on its territory, over its nationals within its territory as well as over non-nationals, including legal persons such as companies within its territory.[27] A State can also exercise jurisdiction over nationals outside its territory on the basis of active or passive

---

[23] Johnson and Post (n 2).

[24] Also see Lawrence Lessig, *Code: Version 2.0* (Basic Books 2006).

[25] Goldsmith (n 2).

[26] For jurisdiction in cyberspace see Kohl (Ch 4 of this Handbook). See also James Crawford, *Brownlie's Principles of Public International Law* (OUP 2012) 456–7; Frederick A Mann, 'The doctrine of international jurisdiction revisited after twenty years' in Academie De Droit International De La Haye, *Recueil Des Cours* (Martinus Nijhoff 1984).

[27] *Nottenbohm Case (Lichtenstein v Guatemala)* [1955] ICJ Rep 4, para 23: Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos,* ECLI:EU:C:2014:317, paras 32–41.

nationality.[28] Passive nationality can, for example, establish jurisdiction in relation to acts of cyber terrorism.[29]

Furthermore, a State can exercise jurisdiction over information circulated through cyberspace at the point of delivery, the point of reception, or when the information crosses through wires and lines falling within its jurisdiction.[30] A State can also exercise jurisdiction over web addresses to the extent they are registered in that State.

More than that, a State can exercise jurisdiction over the effect of cyber acts if they were felt within its territory.[31] The effects doctrine was first enunciated by the Permanent Court of International Justice in the *Lotus* case and since then it has been accepted as a jurisdictional ground.[32] Nonetheless, some questions remain including whether the effects should have been materialised before exercising jurisdiction or whether foreseeable effects can be taken into account;[33] whether the effects should be substantial; or whether they should be detrimental in order to trigger a State's jurisdiction. A particular problem in relation to cyberspace is that cyber effects may be felt in a number of different jurisdictions. If all affected States were to assert jurisdiction, the practical difficulties are considerable. Even if international law contains rules on conflicts of jurisdiction, the assertion of jurisdiction in such situations may affect the principle of fairness. In order to address these issues, certain States require 'substantial contacts'[34] with that State or ascribe to the principle of targeting according to which it is the State targeted by the impugned behaviour that can exercise jurisdiction irrespective of any effects felt in other jurisdictions.[35] That having been said, the effects doctrine is not universally accepted.

A State can also assert its jurisdiction over cyber conduct that endangers its vital interests regardless of where, or by whom, such conduct has been committed.[36] This refers to the protective principle of jurisdiction[37] which provides States with an additional ground to protect themselves against injuries by non-State actors. This would allow, for example, a State to exercise

---

[28] *Arrest Warrant Case (Democratic Republic of Congo v Belgium)* (Joint Separate Opinion of Judges Higgins, Kooijmans and Buergenthal) [2002] ICJ Rep 3, para 47; Restatement of the Law Third, The Foreign Relations Law of the United States (1986) para 402.

[29] *US v Bin Laden*, 92 F.Supp.2d.189 221 (S.D.N.Y., 13 March 2000).

[30] *R v Sheppard & Amor* [2010] EWCA Crim 65; Sean Kanuck, 'Sovereign discourse on cyber conflict under international law' (2010) 88 *Texas Law Review* 1571, 1573–5.

[31] For the effects doctrine see also Kohl (Chapter 4 of this Handbook).

[32] *The Case of the S.S. "Lotus"* (Judgment) [1927] PCIJ Rep Series A No 10 18, para 23; *Arrest Warrant of 11 April 2000* (n 28) para 47.

[33] *U.S. v Yousef*, 327 F.3d 56, 112 (2d Circ, 2003).

[34] *CompuServe, Inc v Patterson* 89 F. 3d 1257 (6th Cir.1996); *Zippo Mfg Co v Zippo Dot Com Inc* 952 F Supp 1119 (WD Pa 1997).

[35] Thomas Schultz, 'Carving up the Internet: Jurisdiction, legal orders, and the private/public international law interface' (2008) 19 *European Journal International Law* 799, 816.

[36] *The Case of the S.S. "Lotus"* (n 32) (Dissenting opinion by Judge Loder) 35–6 (when the 'offences […] are directed against the State itself or against its security or credit [, t]he injured State may try the guilty persons according to its own law if they happen to be in its territory or, if necessary, it may ask for their extradition').

[37] Research on International Law under the Auspices of the Harvard Law School, Part II, 'Jurisdiction with Respect to Crime' (1935) 29 *American Journal International Law* (Supp.) 435, 543; *Attorney-General of Israel v Eichmann* (1961) (District Court), 36 ILR 5 and *Eichmann v Attorney-General* 36 ILR 277 (Supreme Court); Ian Cameron, *The Protective Principle of International Criminal Jurisdiction* (Dartmouth 1994).

jurisdiction over remotely conducted cyber espionage if its security has been compromised. However, the problem with this head of jurisdiction is that the notion of 'essential' or 'vital' State interests is not settled or well-defined.

In sum, a State can assert its sovereignty over the physical layer of cyberspace located on its territory and over information passing through its infrastructure or beginning and ending on its territory. It can also assert its sovereignty over the social layer that is, over all persons on its territory as well as over its nationals outside its territory. A State can finally assert its sovereignty over the effects of cyber activities that are felt within the State or affect its vital interest regardless of their provenance.

The above describe direct assertions of sovereignty by a State but a State can assert its sovereignty also indirectly when the application of its law has 'spill over' effects on cyberspace. For instance, if a State regulates access to certain materials such as pornographic or terrorist materials, it makes their circulation through cyberspace more difficult, although not impossible, in the absence of a common regulatory regime in cyberspace. A State can also do so by globalising the application of its own laws. The dispute between Google and France's *Commission Nationale de l'Informatique et des Libertés* (CNIL) concerning the 'right to be forgotten' that is, the right to remove links containing personal information, is instructive. Google removed material from google.fr and introduced a geoblocking feature to prevent European users from being able to see delisted links whereas CNIL however demanded worldwide delisting. Google appealed to the Conseil d'État which referred the case to the Court of Justice of the European Union for a preliminary ruling.[38] Google argued that such a demand shows 'disregard of public international law's principles of courtesy and non-interference'[39] which are part of the principle of sovereignty. The Court ruled that Google does not have an obligation to comply globally with the EU law on the right to be forgotten, however it did not preclude this possibility. Instead, the Court effectively recognised the competence of national authorities to do so when it opined that:

> a supervisory or judicial authority of a Member State remains competent to weigh up, in the light of national standards of protection of fundamental rights … a data subject's right to privacy and the protection of personal data concerning him or her, on the one hand, and the right to freedom of information, on the other, and, after weighing those rights against each other, to order, where appropriate, the operator of that search engine to carry out a de-referencing concerning all versions of that search engine.[40]

The Court also said that the EU can lay down an obligation of global de-referencing.[41]

The most radical assertion of sovereignty is when States partition cyberspace by creating sovereign cyber zones. For example, China is promoting the principle of cyber sovereignty.[42] In 2010, a White Paper entitled "The Internet in China" was published which stressed the

---

[38] C-507/17, Google Inc v Commision nationale de l'informatique et des libertés (CNIL), Judgment of 24 September 2019 ECLI:EU:C:2019:772.

[39] Ibid., para 37. Although the EU is not a sovereign State, the ruling concerns the General Data Protection Regulation (GDPR) which EU States apply as national law.

[40] Ibid., para 72.

[41] Ibid., para 58. Although the EU is not a State and does not have sovereignty, the point made here is that national laws (including the EU law) can have extraterritorial regulatory scope.

[42] Hao Yeli, 'A Three-Perspective Theory of Cyber Sovereignty' (2017) 17 *Prism: Journal of the Center for Complex Operations* 108; Yi Shen, 'Cyber Sovereignty and the Governance of Global

sovereign implications of the internet.[43] Chinese President Xi Jinping stressed the critical importance of cyber sovereignty to national sovereignty.[44] The protection of sovereignty in cyberspace is also part of China's national security doctrine.[45] The *International Strategy of Cooperation on Cyberspace* released in 2017 states that 'the principle of sovereignty enshrined in the UN Charter covers all aspects of State-to-State relations, which also includes cyberspace'.[46]

China's approach to cyber sovereignty extends to cyber infrastructure under its jurisdiction, over all online activities taking place within Chinese jurisdiction, and over people within China's jurisdiction. In addition to this, sovereignty extends to information entering or becoming available within China's sovereign domain. China asserts its cyber sovereignty in the latter instance through filtering.[47] Filtering involves technical, political, legal, and social techniques to deny access to certain information from within China or deny entry into China of such information. Filtering takes place at the international gateways of Chinese networks and it has been referred to as the 'Great Firewall' of China. Other ways of asserting sovereignty is by requiring international actors such as tech companies to have local presence; requiring foreign tech companies to comply with local laws in order to do business in China; managing domain names; and requiring the local storage of all personal data, including those of non-nationals.

China deploys the principle of cyber sovereignty in order to protect its internal sovereignty that is, its exclusive and supreme power over its territory and people and in order to maintain its freedom in the way it exercises its sovereignty internally.[48] The external dimension of cyber sovereignty aligns with China's demand for equal participation in the international governance

---

Cyberspace' (2016) 1 *Chinese Political Science Review* 81. See also Huang and Ying (Ch 26 of this Handbook).

[43] The Internet in China Information Office of the State Council of the People's Republic of China (2010) https://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm.

[44] 'Why Does Cyber Sovereignty Matter?', *China Daily* (16 December 2015) http://www.chinadaily.com.cn/business/tech/2015-12/16/content_22728202.htm.

[45] Council on Foreign Relations, 'China's New Cybersecurity Law' (2015) https://www.cfr.org/blog/chinas-new-cybersecurity-law.

[46] Ministry of Foreign Affairs of the Peoples Republic of China, International Strategy of Cooperation on Cyberspace (2017) https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml. In its submissions to the second substantive session of the OEWG in 2020, China stated in relation to sovereignty in cyberspace the following:

> States should exercise jurisdiction over the ICT infrastructure, resources as well as ICT-related activities within their territories. States have the right to make ICT-related public policies consistent with national circumstances to manage their own ICT affairs and protect their citizens' legitimate interests in cyberspace. States should refrain from using ICTs to interfere in internal affairs of other states and undermine their political, economic and social stability. States should participate in the management and distribution of international Internet resources on equal footings.

https://www.un.org/disarmament/open-ended-working-group/.

[47] Ron Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain, *Access Denied: The Practice and Policy of Global Internet Filtering* (MIT Press 2008); Ron Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (MIT Press 2010).

[48] According to the International Strategy of Cooperation on Cyberspace:

> China is committed to upholding peace and security in cyberspace and establishing a fair and reasonable international cyberspace order on the basis of state sovereignty, and has worked actively to build international consensus in this respect. China firmly opposes any country using the Internet to interfere in other countries' internal affairs and believes every country has the right and responsi-

of cyberspace which, for China, should be multilateral that is, inter-State. China rejects the multi-stakeholder model of governance where the private sector has equal standing to States and, although it does not reject the participation of non-State actors, their role, in China's opinion, should be secondary.

Another way of asserting sovereignty in cyberspace is by isolating the national internet. For example, countries such as North Korea,[49] Iran,[50] Russia[51] have disconnected or are planning to disconnect national networks from the internet and create national segments of the internet. Such moves are also accompanied by quite far-reaching internal legislation to control information and activities on the national cyber domain such as legislation on blocking and blacklisting, data localisation and access to data, foreign ownership of information providers , encryption and so on. In this way, they can assert their digital sovereignty.

The preceding examples have shown that certain States project a Westphalian concept of State sovereignty to cyberspace. They curve their own sovereign cyberspace by erecting borders through technical means in order to control activities from outside or in order to insulate their national cyber domain. These borders correspond to the borders defining and demarcating territorial sovereignty and, even more critically, they reaffirm sovereignty in its political, social, economic, cultural and territorial dimension. [52] Whether such a Westphalian 'moment' will take hold and lead to the division of cyberspace into sovereign zones depends on many factors. Technology is a critical factor because it can assist in actually curving cyberspace in the same way that the territorial notion of sovereignty was facilitated by tech-

---

bility to maintain its cyber security and protect the legitimate rights and interests of various parties in cyberspace through national laws and policies

International Strategy of Cooperation on Cyberspace (n 46).

[49] Barney Warf, 'The Hermit Kingdom in cyberspace: unveiling the North Korean internet' (2015) 18 *Information, Communication & Society* 109; Saira Asher, 'What the North Korean internet really looks like' (21 September 2016) https://www.bbc.co.uk/news/world-asia-37426725.

[50] 'Iran says its intranet almost ready to shield country from 'harmful' internet' (20 May 20 2019) https://en.radiofarda.com/a/iran-says-its-intranet-almost-ready-to-shield-country-from-harmful-internet/29952836.html.

[51] Robert Morgus and Justin Sherman, 'Analysis: Russia's plans for a national internet', *New America* (19 February 2019) https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/russias-plans-for-a-national-internet/; Timothy Lee, 'Putin signs "Internet sovereignty" bill that expands censorship' (5 February 2019) https://arstechnica.com/tech-policy/2019/05/putin-signs-bill-tightening-government-grip-on-the-russian-internet/; Lily Hay Newman, 'Russia takes a big step toward internet isolation', *Wired* (5 January 2020) https://www.wired.com/story/russia-internet-control-disconnect-censorship/; Alena Epifanova, 'Deciphering Russia's "Sovereign Internet Law" tightening control and accelerating the splinternet', DGAP (German Council of Foreign Relations) Analysis (2020) https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law. Also see Julian Nocetti, 'Contest and conquest: Russia and global internet governance' (2015) 91 *International Affairs* 111; Timothy Thomas, 'Russia's expanding cyber activities: exerting civilian control while enhancing military reform' in Stephen J Blank (ed), *The Russian Military in Contemporary Perspective* (Carlisle Barracks, PA., US Army War College Press 2019) 491–574 and Sayapin (Ch 25 of this Handbook).

[52] According to China's submissions to the UN:

> the free flow of information should be guaranteed under the premises that national sovereignty and security must be safeguarded and that the historical, cultural and political differences among countries be respected; each country has the right to manage its own cyberspace in accordance with its domestic legislation …

UNGA, *Developments in the field of information and telecommunications in the context of international security*, Report of the Secretary-General, UN Doc A/61/161 (18 July 2006) 4.

nological advances, in particular in cartography, which permitted the demarcation of expanses of territory.[53] Beyond technology, there are political, economic, social, and a number of other factors that inform such attempts or consult against such curving. Regardless of how this will pan out, what remains true is that States apply to cyberspace and to cyber activities sovereign configurations of authority and power, albeit with variations and gradations. In view of this, the next question to consider is what is the legal status and import of the principle of sovereignty in cyberspace.

4. THE LEGAL STATUS AND SCOPE OF THE PRINCIPLE OF SOVEREIGNTY IN CYBERSPACE

Although, as explained previously, the importance and place of the principle of sovereignty in international law and in cyberspace is undisputed, recently it has been claimed in relation to cyberspace that sovereignty is just a principle and not a legal rule and, for this reason, it does not engender legal consequences.[54] It has also been claimed that there is no clear State practice and *opinio juris* supporting the view that sovereignty is a rule (compared to political principle) in cyberspace and that the only rules that have legal import in cyberspace are those prohibiting the use of force and intervention.[55]

In response, I argue that the principle of sovereignty is a stand-alone legal principle that applies to cyberspace and produces legal consequences. In order to prove this point, I will first discuss the relationship between 'principles' and 'rules'[56] and, following this, I will discuss the legal status, content, and scope of the principle of sovereignty in international law and in cyberspace.

Principles are general normative propositions containing standards and objectives. They may have political or moral origins but principles become legal when they enter a legal system and translate in legal terms the standards and objectives they represent. Legal principles are also consequential; they produce legal consequences themselves and they may also give rise to more specific rules. Rules are specific proscriptions or prescriptions which individuate specific aspects of the underlying legal principle.

As I explained previously, sovereignty is a fundamental principle of international law. It denotes the aggregate of rights that a State has as a State and vis-à-vis other States.[57] This has

---

[53] Jordan Branch, *The Cartographic State: Maps, Territory, and the Origins of Sovereignty* (CUP 2014).

[54] United Kingdom Attorney General's Office (n 7); Paul C. Ney, Jr, *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference (*2 March 2020) https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/; Gary P Corn and Robert Taylor, 'Sovereignty in the age of cyber' (2017) 111 *American Journal of International Law Unbound* 207. For the opposite view see Harriet Moynihan, 'the application of international law to state cyberattacks: sovereignty and non-intervention' (Chatham House Research Paper, December 2019) https://reader.chathamhouse.org/application-international-law-state-cyberattacks-sovereignty-and-non-intervention?preview=1.

[55] The inclusion of non-intervention, which is usually referred to as a principle, seems to be a contradiction. In my opinion, it strengthens my view that sovereignty is a legal principle as explained in this chapter.

[56] Ronald Dworkin, *Taking Rights Seriously* (Harvard University Press 1978) Chs 2 and 3.

[57] Crawford (n 26) 448.

been affirmed in General Assembly and Security Council resolutions as well as in international instruments.[58] This is also how the ICJ treats sovereignty. In the *Corfu Channel* case the Court held that '[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations' and it went on to say that 'to ensure respect for international law, of which it is the organ, the Court must declare that the action of the British Navy constituted a violation of Albanian sovereignty'.[59] Moreover, sovereignty is a principle that produces legal consequences. In the *Nicaragua case*, the Court held that US overflights violate Nicaragua's sovereignty.[60] In *Costa Rica v Nicaragua*, the ICJ held that by 'excavating three *carios* and establishing a military presence on Costa Rican territory, Nicaragua has violated the territorial sovereignty of Costa Rica'.[61]

Treating sovereignty as a legal principle is not very different from treating it as a 'rule' regarding its legal consequences with the caveat that, as a principle, its normative content is broad and its application is case and context specific in contrast to rules that lead to specific determinations. As a matter of fact, the ICJ uses the concept of legal principle and legal rule interchangeably when referring to certain important principles/rules. In the *Nicaragua* case for example the ICJ treated non-intervention and the non-use of force as both principles and rules.[62] The Court also explained in another case that:

> the association of the terms 'rules' and 'principles' is no more than the use of a dual expression to convey one and the same idea, since in this context 'principles' clearly means principles of law, that is, it also includes rules of international law in whose case the use of the term 'principles' may be justified because of their more general and more fundamental character.[63]

Moreover, according to the Court, a violation of a specific rule such as the rule on the non-use of force can also be a violation of State sovereignty which alludes to what I said above that sovereignty can give rise to specific rules. These rules individuate and protect certain of its elements.[64] Among these rules are, as was said, the rule prohibiting the use of force and the rule prohibiting intervention.[65] The former protects the territorial integrity of a State (an element

---

[58] UNGA Res. 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations (Oct. 24, 1970); Charter of the Organization of American States art. 17, Apr. 30, 1948, 2 U.S.T. 2394, 119 U.N.T.S. 3, art 25.

[59] *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v Albania* [1949] ICJ Rep 35, 36.

[60] *Nicaragua* (n 15) para 251.

[61] *Certain Activities Carried out by Nicaragua in the Border Area (Costa Rica v Nicaragua) and Construction of a Road in Costa Rica Along the San Juan River (Nicaragua v Costa Rica),* 16 December 2015, ICJ Reports 2015, para 229.

[62] *Nicaragua* (n 15) paras 202, 205.

[63] *Delimitation of Maritime Boundary in Gulf of Maine Area (Canada v US)* [1984] ICJ Rep 246, para 79.

[64] France speaks of 'international norms and principles that flow from State sovereignty'; *Droit International Appliqué aux Opérations dans le Cyberespace* (n 7) 1.1.1.

[65] Montevideo Convention (n 18) art 8; United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI, Article 2 (4); *Nicaragua* (n 15*)* paras 202, 204–205; *Case Concerning Armed Activities in the Territory of the Congo (Democratic Republic of the Congo v Uganda)* (Jurisdiction and Admissibility) [2006] ICJ Rep 6, paras 46–48. For a discussion of the non-use of force principle see Rossini (Ch 14 of this Handbook) and for non-intervention see Kilovaty (Ch 5 of this Handbook).

protected by sovereignty) from external aggression, whereas the latter protects the political authority of the State (again an element protected by sovereignty) from external coercion. Because these rules derive from and are linked to sovereignty, I call them 'sovereignist' rules. The emergence of such rules does not however extinguish the principle of sovereignty because its scope is broader than these rules. Instead, sovereignty stands as the background, residual and independent legal principle protecting a State's sovereign rights beyond those protected by any specific rule.

In relation to cyberspace and with the exception of the UK, States that have expressed their views publicly support the view that sovereignty is a stand-alone legal principle that produces legal consequences. For example, Finland has categorically declared that it 'sees sovereignty as a primary rule of international law, a breach of which amounts to an internationally wrongful act and triggers State responsibility'.[66] Likewise, France has affirmed that State sovereignty applies to cyberspace and that cyber operations can violate the principles of sovereignty, non-intervention or the prohibition of the threat or use of force.[67] In the same vein, Iran declared that 'the sovereignty of states is not an extra-legal matter'.[68] The Netherlands declared that 'respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act'.[69] In Estonia's view 'Sovereignty entails not only rights, but also obligations. States are responsible for their internationally wrongful cyber operations just as they would be responsible for any other activity based on international treaties or customary international law.'[70] China stated that 'no infringement of sovereignty in cyberspace will be tolerated'.[71] As the victim of a cyber-attack in 2019, Georgia issued a statement condemning the cyber-attack, 'which goes against international norms and principles, once again infringing Georgia's sovereignty'.[72]

As far as the USA is concerned, its views are quite nuanced. For example, according to the DOD General Counsel 'it does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law' but continues by saying that lawyers should 'take into account the principle of State sovereignty' and that 'States have sovereignty over the information and communications technology infrastructure within their territory'.[73]

From this, it transpires that the main point of contention is not whether sovereignty is legally consequential but what is its scope and content.

In determining its scope and content, it is important to recall what was said previously namely, that sovereignty denotes exclusive and supreme power over territory and people and

---

[66] *International law and cyberspace: Finland's national position* (n 7).

[67] *Droit International Appliqué aux Opérations dans le Cyberespace* (n 7) 1.1 and 1.1.1. For similar views by OAS member States see n 7.

[68] Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace (July 2020) https://www.aldiplomasy.com/en/?p=20901.

[69] Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace Appendix: International law in cyberspace (n 7).

[70] Estonia (n 7).

[71] International Strategy of Cooperation on Cyberspace (n 46).

[72] Statement of the Ministry of Foreign Affairs of Georgia 20 February 2020 available at: https://mfa.gov.ge/News/Statement-of-the-Ministry-of-Foreign-Affairs-o-(7).aspx?CatID=5.

[73] DOD General Counsel Remarks at US Cyber Command (n 54); Egan (n 7).

that it represents the aggregation of rights and duties a State holds as a State and vis-à-vis other States. Thus any non-consensual or not legally justified interference within a State's sovereign legal sphere will constitute violation of its sovereignty.[74] For example, any unauthorised or not legally justified cyber operation on another State's cyber infrastructure which does not reach the level of violence required by the rule on the non-use of force or the level of coercion required by the non-intervention rule will violate the latter State's sovereignty. Otherwise, sovereignty will be denied full legal meaning if its scope and content is to be reduced to those rights protected by the non-use of force and non-intervention rule.[75] Such a view will also create legal and, consequently, responsibility gaps which can be exploited by States.

On the basis of the above it can be said that the Sony attack which involved the hacking and leaking of data from a private company seated in the USA constitutes a violation of US sovereignty because it involved unauthorised entry into US sovereign domain as does the 2019 attack on Georgia which targeted governmental websites and websites of financial institutions, academia and NGOs in Georgia. Likewise, cyber-attacks on hospitals treating COVID-19 patients or information gain operations against R&D facilities in the UK or other States amount to violation of the respective States sovereignty.[76] In contrast, the taking down of the Redatup botnet in 2019 does not violate the principle of sovereignty because the C&C servers that were replaced by French police were situated in France, even if most of the infected computers were outside France. Cyber espionage can also violate a State's sovereignty because it involves operations on foreign networks and indeed operations that exfiltrate or compromise data held in a foreign State's cyber infrastructure without the latter's consent notwithstanding the absence of a specific rule proscribing cyber espionage during peace-time.[77]

An issue that deserves further consideration is whether, in order to constitute a breach of the principle of sovereignty, a cyber operation should reach a certain threshold or produce certain effects. The Tallinn Manual, for instance, mentions certain factors to be taken into account such as death, injury, physical damage, loss of functionality and also speaks of infringements falling below the threshold of loss of functionality.[78] However, it does not indicate the required degree of damage or infringement because they can be quite limited. The Tallinn Manual also mentions 'interference with or usurpation of inherently governmental functions of another State' as another factor to be taken into account but again this refers to the nature of the infringement and not to the degree of infringement. In any case, it should be noted that sovereignty and sovereign rights are not only about governmental functions.

In my opinion, any unauthorised or not legally justified operation that interferes with a State's sovereign rights violates the principle of sovereignty regardless of the degree of interference or damage and regardless of whether it produces physical or non-physical effects

---

[74] *International law and cyberspace: Finland's national position* (n 7) 2–3.

[75] See *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion [1996] ICJ Rep 226, 393–4 (Dissenting Opinion of Judge Shahabuddeen).

[76] NCSC, 'UK and allies expose Russian attacks on coronavirus vaccine development' (16 July 2020) https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development.

[77] See the chapters on cyber espionage by Buchan and Navarrete (Ch 11 of this Handbook) and the use of force by Roscini (Ch 14 of this Handbook). See also Russell Buchan, *Cyber Espionage and International Law* (Hart 2018) 48–69.

[78] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (*CUP 2017) 17–20. See also Moynihan (n 54) paras 51–4.

or whether the operation targets governmental services and infrastructure or not.[79] The harm in this case is normative; it is the harm to the principle of sovereignty and the rights protected by it. It is interesting in this regard to recall France's view that '[a]ny cyberattack against French digital systems or any effects produced on French territory by digital means … constitutes a breach of sovereignty'. France defines cyber-attack as any 'deliberate, offensive and malicious action taken via cyberspace that is intended to cause damage (in terms of availability, integrity or confidentiality) to information or the systems that process it and that may harm the activities of which it or they are the medium'.[80] For France, the principle of sovereignty is violated not only when there are effects but also when there is interference with its information systems since it 'exercises its sovereignty over the information systems located on its territory'.[81] Finland has also taken the same view when it considers as violation of sovereignty '… a non-consensual intrusion in the computer networks and systems that rely on the cyber infrastructure in another State's territory' as well as 'an unauthorized intrusion by cyber means … if it interferes with data or services that are necessary for the exercise of inherently governmental function'.[82]

One could say however that, without any *de minimis* threshold, the principle of sovereignty is trivialised or that the possibility of conflict increases. In response, it can be said that having a *de minimis* threshold does not comport with the importance attached to the principle of sovereignty and with the fact that States may construct their sovereignty differently; some States may adopt an all-inclusive definition covering political, legal, economic, social, cultural aspects, whereas other States may adopt a less inclusive definition of sovereignty. States may also ascribe different degrees of importance to the different values and rights protected by sovereignty. As to whether the absence of any threshold can lead to more conflicts, it can be said that the danger of conflict is more serious if States reject the legal import of the principle of sovereignty and instead interpret the rule on the non-use of force and non-intervention expansively.

What transpires from the above is that the content and scope of the principle of sovereignty cannot be fixed *ab initio* other than in relation to certain core sovereign elements. Consequently, determinations as to whether the principle of sovereignty has been violated should take place on a case by case basis by taking into consideration qualitative and quantitative criteria. This is in fact a common trait of all legal principles namely, that their content and how they apply to a set of facts or situations or legal regimes require interpretation and contextualisation.

Finally, in response to the claim that there is no relevant State practice to support the argument that cyber operations can breach the principle of sovereignty, it should be recalled that States' official pronouncements on the legal status of sovereignty in cyberspace constitute relevant practice and *opinio juris*. It should also be noted that whether a State claims that its sovereignty has been violated is a complex question not only because there is no automatic and independent invocation of illegality in international law but also because a lot depends on

---

[79] See also *International law and cyberspace: Finland's national position* (n 7) 2 ('The situation is the same irrespective of whether such infrastructure belongs to or is operated by governmental institutions, private entities or private individuals').

[80] *Droit International Appliqué aux Opérations dans le Cyberespace* (n 7) 1.1.1.

[81] Ibid. 6.

[82] *International law and cyberspace: Finland's national position* (n 7) 2.

a State's technical capacity to attribute the impugned operation to another State as well as its political will to invoke another State's responsibility. This means that drawing inferences from State practice or silence needs to be more nuanced.

In order to conclude, this section made two main points: first, that sovereignty is a legal principle that applies to cyberspace and produces legal consequences; and, second, that unauthorised interference with a State's sovereign rights in cyberspace constitutes a breach of its sovereignty although such assessments can be made on a case by case basis because the content, scope and application of sovereignty as a principle require interpretation and contextualisation.

5. CYBERSPACE: A SOVEREIGN ENTITY?

In Sections 3 and 4 I examined the question of whether the principle of sovereignty can apply to cyberspace and whether it is legally consequential which I answered in the affirmative. In this section I will examine the question of whether cyberspace itself can be sovereign. The a-territorial and borderless nature of cyberspace may immediately provoke a negative response but, as was said previously, territory is a legal and political construct which is not synonymous with sovereignty. Furthermore, territory is also a social construct; it is about the relationships between humans, activities and spaces and about attachments and allegiances. Also, territory and, more generally, space, is a perception, a cognitive construction.[83] Cyberspace can thus be described as 'the sense of space generated within the mind as we interact with computer technology' and 'the sense of space generated by the computer-user interface, through one or a combination of our senses'.[84] In this respect, it is quite instructive to recall that William Gibson coined the term 'cyberspace' by watching a video game that appeared to cause kids and computer users 'to develop a belief that there is some kind of actual space behind the screen, some place you cannot see but you know is there'.[85] In light of the above, one can say that cyberspace, in addition to its physical, social and logical dimension, it is also a noumenal space 'inhabited' and 'experienced' through machines and virtual interactions by people who are located in real spaces and use physical instruments.[86] These people are the 'netizens' who make up the cyber community.

The question that can immediately be asked is whether 'netizens' can exercise their right to self-determination and declare the sovereignty of cyberspace. In fact, that was what the *Declaration of the Independence of Cyberspace* called for. This may be a possibility in view of the fact that the 'people' who are the subject of the right to self-determination and the institution of the State are distinct entities and also in view of the fact that sovereignty, at least according to contemporary democratic theories, is vested in the people who, on the basis of the

---

[83] Cohen (n 8) 213.

[84] Lance Strate, 'The varieties of cyberspace: Problems in definition and delimitation' (1999) 63 *Western Journal of Communication* 382, 412.

[85] Sue Barnes, 'Cyberspace: Creating paradoxes for the ecology of self' in Lance Strate, Ronald L Jacobson and Stephanie B Gibson (eds), *Communication and Cyberspace* (Hampton Press 1996) 195.

[86] Cohen (n 8) 236.

right to self-determination, have a say in the internal organisation and external representation of the space within which they live.[87]

Whether this is probable in cyberspace and whether such a declaration will have any legal significance or consequences is, however, doubted. In the first place, questions can be asked as to whether 'netizens' constitute a 'people' for self-determination purposes. Although there is no universally accepted definition of the term 'people' in international law, the cyberspace community does not fit any of the different articulations of the term that have been used. For example, a UNESCO report spells out a number of characteristics 'inherent in a description (but not a definition) of a people' which refer to: a common historical tradition; racial or ethnic identity; cultural homogeneity; linguistic unity; religious or ideological affinity; territorial connection; common economic life. The report also notes that 'the group must be of a certain number', that the 'group as a whole must have the will to be identified as a people or the consciousness of being a people' and that the group must have 'institutions or other means of expressing its common characteristics and will for identity'.[88] It immediately becomes apparent that 'netizens' do not satisfy any of the aforementioned indicators such as language, ethnicity and so on but it is their manifestation in the real world that is projected in cyberspace. This also raises the question of how 'netizens' can be differentiated from other communities in order to claim sovereignty. Furthermore, cyber membership is infinite and too heterogeneous to translate into strong consciousness of people-hood beyond certain common interests. Also, the cyber community is broader than the 'netizens'; it is a multi-stakeholder community. However, who are all the stakeholders and what is their stake on the community and on cyberspace are open questions. For instance, tech companies who own and operate cyber infrastructure are part of the cyber community but their interests vary greatly from those of other 'netizens'. Including them in the definition of 'denizens' means that the cyber community will be defined by power differentials at its source which is contrary to the idea of 'people' comprising equal participants.

Even if we move away from such essentialist descriptions of 'people-hood' and consider how the term 'people' has been defined in the post-1945 practice of self-determination, 'netizens' still fall outside such definitions. The 'people' who exercised the right to self-determination and formed their own independent States were those living under colonial rule[89] but 'netizens' cannot claim that they 'inhabit' a territory or a space that is under foreign subjugation or domination. Furthermore, self-determination claims were made and fought on behalf of 'peoples' by groups or individuals who were able to mobilise them and who enjoyed legitimacy, but who among the cyber community can act as a legitimate leader? Moreover,

---

[87] See arts 1(2) and 55 of the UN Charter; art 1 of the International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, 171 (ICCPR) and International Covenant on Economic, Social and Cultural Rights, 16 December 1966, United Nations, Treaty Series, vol. 993, 3 (ICESCR).

[88] UNESCO 'International Meeting of Experts on further study of the concept of the rights of peoples' (22 February 1990) SHS-89/CONF.602/7 para 22; https://unesdoc.unesco.org/ark:/48223/pf0000085152.

[89] Declaration on the Granting of Independence to Colonial Countries and People (14 December 1960) UNGA Res 1514 (XV). See also principle 1 and 5 of the Declaration on Principles of International Law concerning Friendly Relations and cooperation among States in accordance with the Charter of the United Nations, UNGA Res 2625 (XXV) of 24 October 1970. *Case Concerning the Frontier Dispute (Burkina Faso/Republic of Mali)*, 22 December 1986, ICJ Reports 1986, paras 24–25.

who among 'netizens' can rise above their particularistic interests to fight for the political emancipation of cyberspace as a whole?

Finally, if the 'people' who make up the 'netizens' are artificial persons, they are programmed by real persons and lack the generalised intelligence and fully autonomous mind needed for self-awareness, consciousness, deep logic and independent decisions.[90] This means that their claim to self-determination is not fully self-guided but mediated by real humans.

If 'external' self-determination is not possible, can the cyberspace community instead claim internal self-determination? This refers to the post-colonial articulation of the right to self-determination whereby ethnic, religious, linguistic or other groups are granted some form of autonomy and self-rule, albeit within the State.[91] One can say that the 'cyber exceptionalism' thesis mentioned above according to which cyberspace is subject to regulation by its users alludes to this. Yet, said self-regulation is more about private governance than about self-rule and autonomy. Furthermore, there are no claims to autonomy by cyber groups and even offline groups that enjoy the right to internal self-determination have not claimed autonomy in cyberspace.

There are many other reasons why a declaration of sovereignty by 'netizens' is improbable. First, 'netizens' do not suddenly lose their physicality or become displaced figures; they are embodied individuals who live in real spaces which are under State sovereignty. Consequently, any decision to proclaim the sovereignty of cyberspace and any 'laws' or regulations they may promulgate will be subject to scrutiny by the laws of their own State. In fact, such declaration will immediately be declared null and void by States which will use their powers to arrest, try and imprison those individuals. Even if they use encryption, they cannot keep the State out. Secondly, it is the institutional and legal structure of the State that will eventually support cyberspace sovereignty because cyberspace does not have any central authority to promulgate and enforce laws. Put in other words, cyberspace is intermediated by the State and therefore it cannot be sovereign. Thirdly, in relation to the question of whether the cyber community forms a polity where sovereignty can reside, there is no shared feeling among its members that they constitute a political unit based on collective identity and a sense of common destiny upon which the sovereignty of cyberspace can rest. Although 'netizens' may have the consciousness of being cyber users and may share certain common interests, their membership or interactions do not translate into any overriding political, social, legal, or ethical association. Even if cyberspace offers an open and easily accessible public space where questions about common destiny and association can be deliberated and reflected upon, the sheer volume of users and languages and the lack of structures according to which such deliberations can take place and decisions can be made, negate that possibility. In fact, members of the cyber community associate themselves and place their allegiances with their own States and people. The State, even for the cyber community, remains the most legitimate and effective institution to serve human needs, provide protection and secure justice; and remains the only space where popular sovereignty and self-determination can be realised.[92]

---

[90] Of course technology advances and may create such artificial persons emulating human beings but again the question is to what extent they are separated from their creators.

[91] *Reference re Secession of Quebec* [1998] 2 S.C.R. 217.

[92] '[T]he concept of sovereignty satisfies a deep-seated need to protect a society's political identity and self-determination and that this keeps it alive'; Dieter Grimm, *Sovereignty: The Origin and Future of a Political and Legal Concept* (Columbia University Press 2015) 9.

If cyberspace cannot become sovereign because it does not have its own 'people' or polity and does not have its own mechanisms to declare and sustain a claim to sovereignty but all these are intermediated by States and their polities, the immediate question is whether States can attribute sovereignty to cyberspace.

States as the original subjects of international law enjoying full sovereign power can create other entities and delegate their powers but this does not mean that they forfeit their sovereignty. Consequently, even if States were to recognise cyberspace as a separate political entity and endow it with organs and governmental powers such as legislative or judicial powers over issues that hitherto belonged to them, this will not make cyberspace a sovereign entity. As in the case of international organisations, cyberspace will remain circumscribed by State sovereignty.

An issue I will discuss now is whether big tech companies such as Apple, Microsoft, Google or Facebook are in fact sovereign. Often the language used by big tech companies invokes State symbolisms. For example, Brad Smith, the President of Microsoft, said that the tech sector should operate as a neutral digital Switzerland, that 'cyberspace is us', and that 'instead of nation-state attacks being met by responses from other nation-states, they are being met by us'.[93] Another example is the Cybersecurity Tech Accord adopted by tech companies from around the world where they make a number of pledges in order to defend and advance the benefits of the online technologies for society, among which is the pledge to protect users and customers – whether an individual, organisation or government – from cyber-attacks.[94] Above all, it is their power to regulate through their own norms human, social, political, cultural life; enforce their norms through their own institutions and processes; and provide security, a quintessential State function, that makes them State-like entities. Julie Cohen for example opines that such companies are sovereign:[95] they have territories defined by protocols, data flows, and algorithms; they have populations, their users, over whom they exercise authority and power; they practice diplomacy; and they are important participants in the global legal order.[96] This is true to a large extent but it is more about the power of tech companies, financial and otherwise, and about their influence which is a genuine concern for democracies and for the rule of law. However, such power does not make them sovereign in the sense of having full and ultimate

---

[93] Brad Smith, 'The need for a Digital Geneva Convention' (14 February 2017) https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/; Brad Smith, 'Keynote Address at the RSA Conference 2017: The Need for a Digital Geneva Convention' (14 February 2017) 12, https://blogs.microsoft.com/wp-content/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf.

[94] See https://cybertechaccord.org/.

[95] Julie E Cohen, Law for the Platform Economy (2017) 51 *U.C. Davis Law Review* 133, 199–203; Anupam Chander, 'Facebookistan' (2012) 90 *North Carolina Law Review* 1807, 1808.

[96] This includes e.g., meetings between governments and CEOs and other managers. Also, Denmark has appointed a Tech Ambassador who engages in techplomacy. According to the Office of Denmark's Tech Ambassador:

> [t]here are two overall aspects in the operationalization of Techplomacy: (i) Like all other embassies we bring forward concerns or questions on behalf of Danish authorities in a direct and frank dialogue with the tech companies in order to try and influence the direction of technology and our own preparedness. (ii) Influence the international agenda around tech policy questions in accordance with Danish interests and values, including through new alliances, multilateral fora, and multi-stakeholder partnerships.

https://techamb.um.dk/en/.

power as States do; neither is there any transfer of allegiance from States to tech companies.[97] Tech companies are subject to the sovereignty of the State where they operate or are seated and, actually, we are witnessing the gradual curbing of their powers and their subjection to more intense and wide-ranging regulation and scrutiny through legislation, penalties, and judicial enforcement. In short, States assert their sovereignty over tech companies and this is even more evident in authoritarian States.

In order to summarise, it was claimed that cyberspace cannot become sovereign because it lacks the human substratum and autochthonous mechanisms needed to establish and support its sovereignty but instead it is intermediated by States. Also, even if States were to recognise cyberspace as a distinct legal-political entity, this does not make it sovereign. Finally, big tech companies are not sovereign but subject to State sovereignty. That said, I will now discuss a different legal representation of sovereignty in cyberspace.

6. CYBERSPACE AS GLOBAL COMMONS

Cyberspace has sometimes been characterised as a global commons, a *res communis*.[98] The founder of the World Wide Web, for example, dedicated the protocol to the whole world, preventing anyone from attaining property over it.[99] Also, according to the 2017 US National Security Strategy 'the United States will provide leadership and technology to shape and govern common domains—space, cyberspace, air, and maritime—within the framework of international law'.[100]

The global commons concept in international law concerns the type and scope of authority exercised over spaces or, to put it differently, how spaces are governed. Global commons describe resource domains that lie outside States' exclusive sovereignty and are subject to collective use.[101]

---

[97] For example Mark Zuckerberg, Facebook's CEO, envisages 'creating a large-scale democratic process to determine standards with AI to help enforce them'; *Building Global Community* (18 February 2017) https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10103508221158471/. However, previous attempts at direct democracy were unsuccessful; Adi Robertson, 'Mark Zuckerberg wants to democratize Facebook—here's what happened when he tried', *The Verge* (5 April 2018) https://www.theverge.com/2018/4/5/17176834/mark-zuckerberg-facebook-democracy-governance-vote-failure.

[98] Dan Hunter, 'Cyberspace as place and the tragedy of the digital anticommons' (2003) 91 *California Law Review* 439; Abraham M Denmark and James Mulvenon (eds), *Contested Commons: The Future of American Power in a Multipolar World* (Centre for New American Century 2010).

[99] Tim Berners-Lee and Mark Fischetti, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web* (Texere 2000) 124.

[100] *National Security Strategy of the United States* (December 2017) 41, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf; National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age (2018) 34, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf; Mark Barrett *et al*., *Assured Access to the Global Commons* (North Atlantic Treaty Organisation 2011) xii, http://www.alex11.org/wp-content/uploads/2013/01/aagc_finalreport_text.pdf.

[101] UNEP, 'IEG of the Global Commons: Background' (United Nations Environment Programme Division of Environmental Law and Conventions) http://www.unep.org/delc/GlobalCommons/tabid/54404/Default.aspx; John Vogler, 'Global Commons Revisited' (2012) 3 *Global Policy* 61; Mika

The modern concept of global commons has its roots in Roman Law. Roman Law was broadly divided into the law that pertains to persons and the law that pertains to objects (*res*). The latter included both corporeal and incorporeal objects and the law that applied to them depended on their nature and function. Whereas *res in patrimonio* were subject to ownership, *res extra patrimonium* were divided into objects that were subject to divine law and objects that were subject to human law. The latter were further divided into *res communes* (belonging to all mankind); *res publicae* (belonging to a State for use of its citizens); and *res universatis* (belonging to a city for use of its citizens).[102]

Early international lawyers used these Roman Law concepts to describe the legal status and regulation of certain spaces. Grotius characterised the high seas as *res communis* because '… it is so limitless that it cannot become a possession of anyone, and because it is adopted for the use of all, whether considered from the point of view of navigation or of fisheries'. For him, if water is enclosed, it can be subject to possession.[103] In the same vein, Vattel treated the high seas as global commons not subject to appropriation in contrast to areas near the coasts which can be susceptible to ownership.[104]

The modern instantiation of the global commons concept can be found in Article 2 of the Geneva High Seas Convention (1958) and in Articles 87, 89 and 139 of the 1982 United Nations Convention on the Law of the Sea concerning the high seas;[105] in the 1966 Outer Space Treaty in relation to outer space;[106] and in the Antarctic Treaty System which deals with issues of sovereignty and use in Antarctica and defines global commons as 'south of 60 [degrees] South Latitude, including all ice shelves'.[107]

From the spaces designated as global commons it transpires that global commons share certain characteristics which contribute to their legal designation as global commons and their subjection to a system of collective governance in order to enjoy the accrued benefit. They include the accumulated resources of these areas; the indivisibility of assets; the benefits that their exploitation would deliver to each and every State; and the difficulties in apportioning them due to their size and to the fact that their boundaries are not clearly demarcated.

It also transpires that the designation of a space as global commons is not a legal inevitability but depends on broadly defined political considerations that are represented in the legal

---

Aaltola, Joonas Sipilä and Valtteri Vuorisalo, 'Securing global commons: a small state perspective' (FIIA Working Paper 71, June 2011).

[102] Max Radin, 'Fundamental concepts of the Roman Law' (1925) 13 *California Law Review* 207; George Mousourakis, *Fundamentals of Roman Private Law* (Springer 2012) 119–21.

[103] Hugo Grotius, *The Freedom of the Seas, or, the Rights which Belongs to the Dutch to take part in the East Indian Trade* (edited by James B Scott, OUP 1916) 28. See further Hugo Grotius, *The Classics of International Law: De Jure Belli Ac Pacis Libri Tres*: *Vol. II Book II* (translated by Francis W Kelsey *et al*, Clarendon/Carnegie Endowment for International Peace 1925) Ch II para III.

[104] Emer Vattel, *Le Droit Des Gens ou Principes de la Loi Naturelle, appliques à la Conduite et aux Affaires des Nations et des Souverains* (Liberty Fund 2008) Ch XXIII, 125–7.

[105] United Nations Convention on the Law of the Sea (signed 10 December 1982, entered into force 16 November 1994).

[106] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (19 December 1966) arts 1, 2, 7, 8.

[107] *The Antarctic Treaty* (signed 1 December 1959, entered into force 23 June 1963) Articles IV, V and VI. It can be said however that Antarctica is not a global commons *stricto sensu*. See Silja Vöneky and Sange Addison-Agyei, 'Antarctica' in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (2011) para 19.

concept of global commons. States can still extend their authority over the designated area if they wish but, for the reason explained above, States agree to refrain from claiming ownership over that area and agree to exercise their authority concurrently with that of other States. For this reason, they devise a common regulatory regime to fulfil the designation of the referent area as global commons.

This indicates that the global commons concept is a legal-political construct which is not adverse to the principle of sovereignty. When States decide to designate a certain area as global commons and, consequently, agree to abstain from exercising their full sovereignty over such an area, this is an act of sovereign authority. Auto-limitation is an expression of sovereignty. As the PCIJ said in the *S.S. Wimbledon* case: 'The Court declines to see, in the conclusion of any treaty by which a State undertakes to perform or refrain from performing a particular act, an abandonment of its sovereignty … the right of entering into international engagements is an attribute of State sovereignty.'[108]

All this means that cyberspace can in principle be designated a global commons if States agree to do so and subsequently design the rules and principles to govern that area. However, at this point in time, there is no political or legal impetus to do so and whether such impetus will emerge depends on many variables – political, legal, social, cultural – but the underlying question is whether cyberspace warrants to be so designated if compared to existing global commons. In this regard it should be noted that, although cyberspace exhibits some of the characteristics of global commons, for example borderless, there are also important differences between cyberspace and other global commons. First, whereas global commons refer to natural resources and have a physical dimension, cyberspace is a technical, man-made, resource domain which also has a virtual dimension. Second, global commons have outward physical and geographical boundaries which delineate the space, however, this is not the case in cyberspace where its virtual part permeates all boundaries whereas its physical part in the sense of infrastructure and humans falls within State boundaries. Third, whereas global commons are created in order to avoid depletion of natural resources, this is not the case in cyberspace where resources cannot be depleted naturally but expanded or depleted technically.[109] Fourth, whereas global commons are non-excludable in the sense that others cannot be excluded, the extent that cyber infrastructure belongs to States means that others can be excluded as was mentioned above. Finally, the physical part of cyberspace, such as computers, is under national jurisdiction and in most cases it is privately owned which means that it should be 'de-owned' in order for cyberspace to form a global commons but this would be legally difficult. It is for these reasons that cyberspace was at best described as an 'imperfect commons'.[110]

---

[108] *S.S. 'Wimbledon'* (Judgment of 17 August 1923) [1923] PCIJ Rep Series A No 1, 25.

[109] This relates to Hardin's 'tragedy of the commons'; see Garrett Hardin, 'The tragedy of the commons' (1968) 162 *Science* 1243.

[110] Joseph S Nye, *The Future of Power* (Public Affairs Press 2011) 143; James A Lewis, 'Sovereignty and the role of government in cyberspace' (2010) 16 *Brown Journal of World Affairs* 55, 62.

7. CONCLUDING THOUGHTS

It has become apparent from the preceding discussion that cyberspace has not acquired any special legal status in international law but, instead, existing legal categories and principles such as the principle of sovereignty have been applied to cyberspace and are used to explain its legal status. The chapter has also shown that the principle of sovereignty is not only a stand-alone legal principle but also that it produces legal consequences. In other words, there is definitely a sovereignty redux in cyberspace. This does not however mean that there are no disputes about its scope and content or that no further clarifications are needed. But this is what principles require; they require interpretation and contextualisation.

One may ask why sovereignty, which as was said is the engine behind the creation of international law, has not produced a global and comprehensive regulatory regime for cyberspace. In response, it should be said that law-production is not an inevitable outcome of sovereignty because sovereignty can also thwart the international law-production process. Yet, if States' sovereign interests and needs begin to coalesce around certain issues, sovereignty can generate new law.[111] Although this seems to be unattainable at this point in time, the principle of sovereignty applies and will continue to apply in cyberspace shaping and rationalising State behaviour and the international rules that apply or will apply in the future to cyberspace.

[111] Nicholas Tsagourias, 'The slow process of normativizing cyberspace' (2019) 113 *American Journal of International Law Unbound* 71.

2. The rise of cyber norms

Marja Lehto[1]

1. INTRODUCTION

Norms have recently acquired a prominent standing in the area of international cybersecurity.[2] This turn has been influenced by several developments, both global and regional, public and private. In particular, the adoption in 2015 by a United Nations Group of Governmental Experts (GGE) of a list of 'norms, rules and principles for responsible behavior of States in the use of ICTs' (information and communication technologies) can be regarded as a milestone.[3] No less than three UN groups – two new GGEs and an open-ended working group – have subsequently been mandated to further discuss and develop such norms.[4] The UN process has also triggered other initiatives, which have resulted in the formulation of cybersecurity norms, most notably by the Global Commission on Stability in Cyberspace[5] and the Paris Call for Trust and Security in Cyberspace.[6] The private sector has put forward cyber norms of its own, including norms regarding State behaviour. Microsoft may be the best-known example of corporate entities having actively participated in the cyber norms debate addressing both States and private actors.[7] Civil society actors have also contributed to the development and

[1] The views expressed in the chapter do not necessarily reflect those of the MFA. All websites last accessed on 3 December 2020.

[2] See e.g., Martha Finnemore and Duncan B Hollis, 'Constructing norms for global cybersecurity' (2016) 110 *American Journal of International Law* 425.

[3] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015 report, UN Doc. A/70/174 (GGE 2015 report).

[4] UN Doc. A/RES/70/237, Developments in the field of information and telecommunications in the context of international security, para 5; UN Doc. A/RES/73/266, Advancing responsible State behavior in cyberspace in the context of international security, para 3; UN Doc. A/RES/73/27, Developments in the field of information and telecommunications in the context of international security, para 5.

[5] Global Commission on the Stability of Cyberspace (GCSC), *Advancing Cyberstability*, Final Report, November 2019. See also GCSC, *Norms through Singapore*, November 2018.

[6] Paris Call for Trust and Security in Cyberspace (2019) https://pariscall.international/en/principles.

[7] See Microsoft, *Five Principles for Shaping Cyber Security Norms* (2013), *International Cybersecurity Norms: Reducing Conflict in an Internet-dependent World (2014)* and *Digital Geneva Convention to Protect Cyberspace* (2017). See Maria Gurova, *The Proposed 'Digital Geneva' Convention*, Geneva Centre for Security Policy, Strategic security Analysis 4/2017 and Valentin Jeutner, 'The Digital Geneva Convention: A critical appraisal of Microsoft's proposal' (2019) 10 *Journal of International Humanitarian Legal Studies* 158. In 2018, Microsoft proposed a 'Cybersecurity Tech Accord' which has since then attracted the accession of more than 70 enterprises. All Microsoft proposals are available at https://www.microsoft.com. Siemens presented in 2018 together with eight other corporations a 'Charter of Trust for a Secure Digital World', available at https://assets.new.siemens.com/siemens/assets/api/uuid:9bbe02e9-fcb2-4948-9977-a668cac52e50/version:1567432347/charter-of-trust-presentation-en-20190902-website.pdf.

analysis of cyber norms.[8] Cybersecurity norms have been deemed to constitute 'the preferred regulatory vehicle for advancing the stability and safety of cyberspace'.[9]

The GGE norms outline the basic principles for 'responsible State behaviour' in cyberspace and are thus addressed exclusively to States. They include both norms calling for reinforced inter-State cooperation and those requesting States to take appropriate measures domestically to strengthen cybersecurity. Examples of the former include recommendations for cooperation in the prevention of harmful ICT practices, exchange of information, and consultations in the event of malicious cyber incidents.[10] Norms of the latter type seek to enhance the protection of critical infrastructures,[11] ensure the integrity of supply chain,[12] and increase information of ICT vulnerabilities and available remedies.[13] Even though the two last-mentioned tasks may only be implemented in close cooperation with the private sector, the norms focus on States, asking them to 'encourage responsible reporting of ICT vulnerabilities' and 'take reasonable steps to ensure […] that end users can have confidence in the security of ICT products'.[14] In addition to such prescriptive norms, the 2015 GGE list includes norms of restraint based on the existing international obligations of States.[15]

The eight norms put forward by the Global Commission on the Stability of Cyberspace, while also seeking to strengthen the stability of cyberspace, are different from the GGE norms in that they address both States and non-State actors. The norms common to both categories of addressees seek to protect the public core of the internet and the integrity of electoral infrastructures as well as to prevent tampering with products or services, and the commandeering of ICT devices as botnets. In addition, other norms seek to increase information on vulnerabilities and ensure that the basic standards of cyber hygiene are observed by States. Finally, one norm seeks to ensure that offensive cyber operations in cyberspace are reserved solely to States.[16] The Paris Call, too, is open for endorsement by both States and non-State actors. Its nine broad principles address very much the same questions as the report of the Global Commission from protection of the public core of the internet to defence of electoral processes, supply chain integrity, non-proliferation and prevention of private hack-back. In addition, they deal with the

---

[8] See, for instance, Paul Meyer, *Global Cyber Security Norms: A Proliferation Problem?*, ICT for Peace Foundation (2015). Further information of the activities of ICT for Peace is available at https://www.ict4peace.org. See also *Promoting International Cyber Norms: A New Advocacy Forum*, A Report from the East-West Institute Breakthrough Group on Promoting Measures of Restraint in Cyber Armaments, East-West Institute 2015. For the East-West Institute's program on Global Cooperation in Cyberspace, see https://www.eastwest.ngo/pillars/global-cooperation-cyberspace. See also Eneken Tikk (ed), *Voluntary, Non-binding Norms for Responsible State Behaviour in the Use of Information and Communication Technology, A Commentary*, Civil Society and Disarmament, United Nations Office for Disarmament Affairs (UNODA) (2017).

[9] Finnemore and Hollis (n 2) 436. Similarly, Camino Kavanagh, *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century*, UNIDIR (2017) 10.

[10] GGE 2015 Report (n 3) paras 13(a), 13(d) and 13(h).

[11] Ibid., para 13(g).

[12] Ibid., para 13(i).

[13] Ibid., para 13(j).

[14] Ibid., paras 13(j) and 13(i).

[15] Ibid., paras 13(c), 13(f) and 13(k).

[16] GCSC, *Advancing Cyberstability* (n 5) 28.

prevention of ICT-enabled theft of proprietary information and intellectual property, as well as coordinated disclosure of ICT vulnerabilities.[17]

The GGE list of 'norms, rules and principles for responsible State behaviour' stands out among the different sets of norms because of its wide endorsement by States as a roadmap for greater cybersecurity. Once adopted by the group of 20 governmental experts, the norms have been welcomed and endorsed by the UN General Assembly, which has recommended them as guidance to States.[18] The list of norms has subsequently been incorporated in a General Assembly resolution.[19] Beyond the United Nations, the European Union (EU), the Group of Seven (G7), the Group of 20 largest economies (G20) as well as the Association of Southeast Asian Nations (ASEAN) have endorsed the list of norms, either referring to them or incorporating them in their declarations.[20] The EU has moreover developed specific instruments, a Cyber Diplomacy Toolbox[21] as well as a regime of cyber sanctions[22] with the intention of upholding and implementing respect for international law and responsible State behaviour in cyberspace. The 2015 list of norms also marked the culmination point of the GGE process that had been initiated in 2004.[23] The failure of a subsequent group of governmental experts to adopt a report in 2017[24] has only underlined the importance of the 2015 *acquis*.

This chapter addresses the turn to cyber norms with a specific focus on the 2015 GGE list of norms, which has become a point of reference for responsible State behaviour in cyberspace. Other proposed norms are referred to when there is a particular reason to do so. The analysis of the GGE norms also gives reason to look more closely at the concept of 'norm' as well as at the relationship between non-binding normative instruments and international law. These issues are addressed both generally and in relation to the negotiation history and content of the GGE norms. The discussion of the nature of the 2015 norms is completed with an overview of the follow-up given to them so far.

---

17 Paris Call (n 6).

18 UN Doc. A/RES/70/237, paras 1 and 2(a).

19 UN Doc. A/RES/73/27, para 1.

20 EU Council conclusions on malicious cyber activities, 16 April 2018, No. 7925/18; G7 Declaration of Responsible State Behavior, Lucca (11 April 2017) http://www.g7italy.it/en/meeting/foreign-affairs/index.html; G20 Leaders' Communiqué, Antalya Summit (15–16 November 2015) https://www.gpfi.org/publications/g20-leaders-communiqu-antalya-summit-2015; ASEAN Leaders' Statement on Cybersecurity Cooperation, 2nd ASEAN Ministerial Conference on Cybersecurity (2017) http://setnas-asean.id/site/uploads/document/document/5b04cdc25d192-asean-leaders-statement-on-cybersecurity-cooperation.pdf.

21 Framework for a joint EU Diplomatic Response to Malicious Cyber Activities (Cyber Diplomacy Toolbox), 9916/17 (7 June 2017). The toolbox refers, in paras 2 and 3, to the 2010, 2013 and 2015 reports of the UN GGE and encourages the member States to 'be guided by the UN GGE reports' recommendations in their use of ICTs'.

22 Council Decision (CFSP) 2019/797 (17 May 2019) concerning restrictive measures against cyber-attacks threatening the Union or its Member States, recital 4 refers to the GGE work. See also Patryk Pawlak and Thomas Biersteker (eds), *Guardian of the Galaxy. EU cyber sanctions and norms in cyberspace*, Chaillot Paper 155 (October 2019).

23 UNODA, *Fact-sheet: Developments in the field of Information and Telecommunications in the context of International Security*, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf.

24 See Eneken Tikk and Mika Kerttunen, *Parabasis. Cyber-diplomacy in Stalemate*, Norwegian Institute of International Affairs, NUPI Report 5/2018.

2. THE CONCEPT OF 'NORM'

Considerable attention has been paid in international law research to the phenomenon of non-binding normative instruments. The dominant perspective relates to the role that such instruments play in international law-making. Maybe for this reason, the term of art is 'soft law'[25] rather than 'norm', the latter term being most often used to refer to legal rules and principles. In contrast, international relations scholarship has paid special attention to the concept of norm detached from the legal context, also reflected in several recent comments on cyber norms.[26] A norm in this sense is understood to set forth 'collective expectations for the proper behavior of actors with a given identity'.[27] A key characteristic of this kind of a norm is that it is widely accepted and internalised in the relevant community. Regulations not meeting this requirement, even if labelled as norms, are but 'normative aspirations', or 'quasi-norms'.[28] Shared understandings regarding right and wrong conduct may be established over time by those who participate in particular practices, or be actively promoted by 'norm entrepreneurs'.[29] The nature of such norms as broad social constructions, and the need for internalisation, is evident from the language used to describe them, for instance references to 'cultivating international cyber norms'[30] and the requirement that a norm 'needs to resonate within a community to take root'.[31] The emergence, application and further development of norms is furthermore conceived as a continuing process.[32]

While this view of norms shares certain commonalities with the established concept of customary international law as 'unwritten law deriving from practice accepted as law'[33] and has inspired reflection and analysis on the process in which international legal obligations emerge,[34] the perspective is different. Most importantly, the legally binding nature of a reg-

---

[25] See Dinah Shelton, 'Soft law' in David Armstrong, Jutta Brunnée, Michael Byers, John H Jackson and David Kennedy (eds), *Handbook of International Law* (Routledge 2008); Alan Boyle and Christine Chinkin, *The Making of International Law* (OUP 2007).

[26] Martha Finnemore, 'Cultivating international cyber norms' in Kristin M Lord and Travis Sharp (eds), *America's Cyber Future: Security and Property in the Information Age* (Center for a New American Security 2011); Finnemore and Hollis (n 2); Xymena Kurowska, *The Politics of Cyber Norms: Beyond Norm Construction Towards Strategic Narrative Contestation*, EU Cyber Direct (March 2019).

[27] Peter J Katzenstein, 'Introduction: Alternative perspectives on national security' in Peter J Katzenstein (ed), *National Security: Norms and Identity in World Politics* (Columbia University Press 1996) 5. See also Martha Finnemore and Kathryn Sikkink, 'International norm dynamics and political change' (1998) 52 *International Organization* 887, 917 ('[a] standard of appropriate behaviour for actors with a given identity'); Annika Björkdahl, 'Norms in international relations: Some conceptual and methodological reflections' (2002) 15 *Cambridge Review of International Affairs* 9.

[28] Toni Erskine and Madeline Carr, 'Beyond "Quasi-Norms": The challenges and potential of engaging with norms in cyberspace' in Anna-Maria Osula and Henry Rõigas (eds), *International Cyber Norms Legal, Policy and Industry Perspectives* (CCDCOE Publications 2016) 100.

[29] Ibid., 102. See also Finnemore and Hollis (n 2) 445–53.

[30] Finnemore (n 26).

[31] Kurowska (n 26) 3.

[32] Finnemore and Hollis (n 2).

[33] International Law Commission, Draft Conclusions on Identification of Customary International Law, General commentary, para 3, *Report of the International Law Commission of the seventieth session* (2018), UN Doc. A/73/10, 122.

[34] See, e.g., Jutta Brunnée and Stephen Toope*, Legitimacy and Legality in International Law: An Interactional Account* (CUP 2010).

ulation, or lack of it, is of no consequence to the international relations conception of norm. Norms may be overlapping with existing international law – 'laws can serve as a basis for formulating norms, just as norms can be codified in law'[35] – but this is not necessarily the case. It is also conceivable, as Erskine and Carr have pointed out, that a legal rule or principle might not constitute a norm in the sense of a social norm 'if it is neither internalized by, nor informs the behaviour of those to whom it is meant to apply'.[36] From the point of view of international law, however, the dichotomy binding/non-binding, or *lex lata* and *lex ferenda*, cannot be overlooked.[37] An essential difference between an international norm that merely acts as a point of reference for expected behaviour, and an international legal norm, is that a violation of the latter entails international responsibility and may be subject to legal enforcement mechanisms.[38]

It is not rare that normative statements are included in non-binding instruments and may contribute to the formation of both customary and treaty law. A classical example, the UN General Assembly's resolutions, which according to the UN Charter have the status of recommendations,[39] may sometimes be evidence of existing international law, or contribute to the formation of new customary international law.[40] In the past few decades, it has become increasingly common that States make use, also outside the United Nations, of declarations, guidelines, codes of conduct, plans of action or other such instruments to give expression to normative commitments and statements of expected behaviour. On some occasions, similar or more specific commitments have been subsequently established in treaty form. Such developments are well-known in various fields of international law, for instance in international human rights law, international environmental law, and the law of the outer space. A pertinent example is given by the nine general principles set out in the 1963 Outer Space Principles Declaration,[41] which were later included in the Outer Space Treaty with only minor modifications.[42] Non-binding commitments can also be an integral part of international law-making, like in the case of the 1948 Universal Declaration of Human Rights,[43] which laid the basis for the two Human Rights Covenants[44] and has been referred to in most of the subsequent human

---

35 Finnemore and Hollis (n 2) 442.

36 Erskine and Carr (n 28) 91.

37 See Jan Klabbers, 'The redundancy of soft law' (1996) 65 *Nordic Journal of International Law* 167 and Jan Klabbers, 'The undesirability of soft law' (1998) 67 *Nordic Journal of International Law* 381.

38 Of the importance of this distinction for the cyber norms debate, see Anna-Maria Osula and Henry Rõigas, 'Introduction' in Osula and Rõigas (n 28) 12. See also Michael N Schmitt and Liis Vihul, 'The nature of international law cyber norms' in Osula and Rõigas, ibid.

39 Charter of the United Nations, San Francisco, 26 June 1945, United Nations, *Treaty Series*, Chapter 1:1, art 13.

40 International Law Commission, Draft Conclusions on Identification of Customary International Law (n 33) Conclusion 12, para 2 and commentary.

41 Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space, UN Doc. A/RES/1962(XVIII).

42 Steven Freeland, 'The role of "Soft Law" in Public International Law and its relevance to the International Legal Regulation of Outer Space' in Irmgard Marboe (ed), *Soft Law in Outer Space: The Function of Non-binding Norms in International Space Law* (Bohlau Verlag Gmbh & Cie 2012) 25.

43 Universal Declaration of Human Rights, UN Doc. A/RES/217 A.

44 International Covenant on Civil and Political Rights, 19 December 1966, United Nations, *Treaty Series*, vol. 999, 171; International Covenant on Economic, Social and Cultural Rights, 16 December 1966, United Nations, *Treaty Series*, vol. 993, 3.

rights conventions. Similarly, the 1972 Stockholm Declaration of Human Environment[45] and the 1992 Rio Declaration on Environment and Development [46] have been generally recognised as the cornerstones of the subsequent development of international environmental law.

At the same time, non-binding commitments come in different forms and serve different purposes. According to Shelton, a non-binding normative instrument may codify pre-existing customary international law, crystallise a trend towards a particular norm, or precede and help form new customary international law. In relation to existing treaties in force, non-binding instruments may fill in gaps in such treaties or form part of the subsequent State practice for the purposes of treaty interpretation.[47] Non-binding instruments may furthermore provide authoritative interpretation of an existing treaty, or build on and add detail to its provisions. Several landmark resolutions of the UN General Assembly have authoritatively interpreted the provisions of the UN Charter,[48] and environmental treaties have often been complemented by guidelines or technical standards that add specificity to their broad formulations and provide for easy updating.[49] In addition to such clearly legal functions, non-binding instruments may consolidate political opinion around the need for action on a new problem, provide guidance or a model for domestic laws, and, finally, 'substitute for legal obligations when on-going relations make formal treaties too costly and time-consuming or otherwise unnecessary or politically unacceptable'.[50]

3. ABOUT THE GGE NORMS: INTENT

Whether a particular non-binding document is capable of contributing to the formation of international law depends primarily on its content and the intention of its drafters.[51] Both aspects are relevant with regard to the GGE's 2015 list of 'norms, rules and principles'.[52] An obvious point of departure for assessing the intention of the drafters of the list is the consistent description in several preceding paragraphs of the norms as 'voluntary and non-binding'.[53] At the same time, the 2015 GGE report is a compromise between competing ambitions, which presents a certain amount of deliberate ambiguity.[54] It is difficult, for instance, to overlook that

---

[45] *Declaration on the Human Environment*, in Report of the United Nations Conference on the Human Environment, 16 June 1972, A/CONF.48/14, at 2 and Corr.1.

[46] *Rio Declaration on Environment and Development*, 12 August 1992, A/CONF/151/26 (vol. 1).

[47] Shelton (n 25) 72; see also *Vienna Convention on the Law of Treaties*, United Nations, *Treaty Series*, vol. 1155, 331, art 31(3)(b).

[48] See e.g., *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, UN Doc. A/RES/2625 (XXV) (Friendly Relations Declaration).

[49] Boyle and Chinkin (n 25) 218.

[50] Shelton (n 25) 72.

[51] Boyle and Chinkin (n 25) 213.

[52] The title may be taken to indicate that the list contains three different types of provisions. It is nevertheless difficult to distinguish between 'norms', 'rules' and 'principles', and the GGE itself has made no attempt to do so. In subsequent comments, references have mainly been made to the composite concept of 'norms, rules and principles' or simply to 'norms'.

[53] UN Doc. A/70/174, paras 9, 10, and 13 (chapeau).

[54] Erskine and Carr (n 28) 96, point out as challenges to a normative development in cyberspace, inter alia, competing value systems and understandings of the relationship between privacy, transparency

some of the norms are based on existing international law. The negotiation process, furthermore, reveals different understandings of the phrase 'norms, rules and principles'.

Apart from the three reports adopted by the Group of Governmental Experts in 2010, 2013 and 2015, no *travaux préparatoires* are available to shed light on the GGE negotiation process. The 2010 report is procedural in nature and only recommends 'further dialogue among States to discuss norms pertaining to State use of ICTs'.[55] While it provides no additional explanation on how the term 'norm' should be understood,[56] a subsequent report adopted in 2013 contains a whole section on 'norms, rules and principles of responsible behaviour by States'. According to its opening paragraph, this section deals with 'norms *derived from existing international law* relevant to the use of ICTs by States'.[57] The text goes on to note that reaching common understandings on how such norms shall apply to State use of ICTs would require further study. Furthermore, '[g]iven the unique attributes of ICTs, additional norms could be developed over time'.[58] A plausible interpretation of these sentences is that, first, the relevant norms have their basis in existing international law and, second, there is a need to study how international law applies in cyberspace. At the same time, the door is left open for further legal developments should that be deemed necessary.[59] A number of international law issues, such as State sovereignty,[60] human rights,[61] harmonisation of legal approaches to criminal or terrorist use of ICTs,[62] State responsibility,[63] and the applicability of international law in cyberspace[64] are addressed in the norms section.

The 2015 report opens a different perspective to the discussion of norms. Most remarkably, it separates the concept 'norms, rules and principles' from that of international law and specifies that the former are 'voluntary and non-binding'. Sovereignty, human rights and other questions of international law are discussed under the title 'how international law applies to the

---

and anonymity, which 'generate tension around differing perceptions of "security" in cyberspace'. See also Alex Grigsby, 'The end of cyber norms' (December 2017–January 2018) 59 *Survival* 109, 110.

[55] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2010 report, UN Doc. A/65/201, para 18(i), 8.

[56] Anna-Maria Osula and Henry Rõigas, 'Introduction' in Osula and Rõigas (n 28) 14 ('throughout the report, it remains unsettled whether the "norms" discussed are legally or politically binding').

[57] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013 report, UN Doc. A/68/98 (GGE 2013 report) para 16, emphasis added.

[58] Ibid.

[59] Similarly Grigsby (n 54) 112.

[60] GGE 2015 report *(*n 3) para 20 ('[T]he applicability of State sovereignty and international norms and principles that flow from sovereignty to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory').

[61] Ibid., para 21 ('State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments').

[62] Ibid., para 22 ('States should intensify cooperation against criminal or terrorist use of ICTs, harmonize legal approaches as appropriate and strengthen practical collaboration between respective law enforcement and prosecutorial agencies').

[63] Ibid., para 23.

[64] Ibid., para 19 ('International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment').

use of ICTs'. Even when referring to previous GGE reports, the 2015 report's norms section omits a reference to international law speaking simply of 'existing norms and commitments'.[65] The difference to the thinking of 2013 is also evident in the last indent of the list of 'norms, rules and principles' which reproduces the 2013 statement '[g]iven the unique attributes of ICTs, additional norms could be developed over time'. While this sentence in the 2013 report seems to serve as a placeholder for further legal developments, the 2015 report refers exclusively to further non-binding norms. According to Tikk, this shift in how the concept of norm is understood has generated some confusion in the GGE discussion of cyber norms.[66]

4. ABOUT THE GGE NORMS: CONTENT

As regards the content of the 11 GGE norms set forth in the 2015 report, it is obvious that the list contains different types of provisions. Those most readily complying with the characterisation of being 'voluntary and non-binding' include a number of norms seeking to reinforce cooperation between States in the interest of increasing stability and security in the use of ICTs,[67] in countering terrorist and criminal use of ICTs,[68] and regarding assistance in the event of malicious cyber-attacks against critical infrastructure.[69] Furthermore, some of the norms concerning measures that States are expected to take domestically[70] can be taken as recommendations in the sense of not corresponding to existing international obligations. It should nevertheless be added that the call on States 'to cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are harmful or may pose threats to international peace and security'[71] is not completely detached from such obligations.[72] Similarly, the norm regarding exchange of information and assistance to address terrorist or criminal use of ICTs may relate to obligations under existing counter-terrorist or other criminal law conventions.[73] The links that the other above-mentioned norms, whether promoting inter-State cooperation or seeking to enhance national resilience, may have with international legal obligations are less clear. This is also true for a further norm referring to the challenges of attribution in cyberspace and recommending caution in the event

---

65 Ibid., para 11.
66 Eneken Tikk, 'Introduction' in Tikk (n 8) 3–4.
67 2015 GGE Report (n 3) para 13(a).
68 Ibid., para 13(d).
69 Ibid., para 13(h).
70 E.g. those calling on States to take measures to protect their critical infrastructure, to encourage responsible reporting of ICT vulnerabilities, to ensure the integrity of the supply chain so that end users have trust in ICT products and to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.
71 2015 GGE Report (n 3) para 13(a).
72 United Nations Charter, arts 1(1) and 3; UN Doc. A/RES/2625(XXV), Friendly Relations Declaration (n 48).
73 International Law Association, Study Group on Cybersecurity, Terrorism, and International Law, Report (31 July 2016) paras 99–101 and more specifically paras 102–23. One of the recommendations of the report is to better utilize existing international law in countering cyberterrorism, see para 334. See also the Council of Europe Cybercrime Convention, ETS No. 185.

of ICT incidents, which has been phrased in a way that does not make its normative nature obvious.[74]

The remaining norms are more closely related to existing legal rights or obligations of States. A norm concerning human rights,[75] for instance, makes express reference to a number of Human Rights Council[76] and UN General Assembly[77] resolutions, which on their turn draw on various Human Rights Conventions and the jurisprudence of human rights treaty bodies. A detailed analysis of these resolutions reveals the broad scope of the norm.[78] It does not only cover the statement that 'the same rights that people have offline must be protected online', but also refers to a number of specific aspects relevant to the right of privacy and the freedom of expression, as well as to promoting and facilitating access to the Internet.[79] As the norm does not add anything to the resolutions it enumerates, the underlying legal instruments, or the interpretative practice by treaty bodies, however, it must be taken as a mere reminder of existing obligations. According to a further norm States should not 'conduct or knowingly support activity to harm the information systems of the authorized emergency response teams of another State' and not use such teams 'to engage in malicious international activity'.[80] This norm seems to rely on the general obligation of States to refrain from harmful activity that may violate the sovereignty of other States or amount to a breach of other international obligations, giving them a cyber-specific amplification. Whether compliance with such obligations should be presented as voluntary in cyberspace, is nevertheless questionable.

A few norms raise more intricate questions regarding their relationship with international law. A case in point is provided by the norm paraphrasing the established principle that it is 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'.[81] Based on the Roman maxim *Sic utere tuo ut alienum non laedas* (use your own property in such a manner as not to injure that of another), this principle is a corollary to State sovereignty. It has been codified in a number of specific branches of international law and is widely understood to constitute a general principle applicable to all State activities.[82] The 2013 GGE report, in stating that 'State sovereignty as well as the norms and principles flowing from sovereignty apply to state conduct of ICT-related activities and to

---

[74] GGE 2015 report (n 3) para 13(b) ('In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences').

[75] Ibid., para 13(e).

[76] UN Doc A/HRC/RES/20/8, *The promotion, protection and enjoyment of human rights on the Internet*, 16 July 2012; UN Doc A/HRC/RES/26/13, *The right to privacy in the digital age* (14 July 2014).

[77] UN Doc. A/RES/68/167, 18 December 2013, and UN Doc. A/RES/69/166, 18 December 2014, both on *The right to privacy in the digital age*.

[78] For such an analysis, see Barrie Sander, 'Recommendation 13(e)' Tikk (n 8) 95–168.

[79] Ibid.

[80] GGE 2015 report (n 3) para 13(k).

[81] *Corfu Channel case,* Judgment of April 9th [1949] ICJ Rep 4, 22 (*Corfu Channel case*).

[82] International Law Commission, Draft Articles on the Prevention of transboundary harm from hazardous activities, art 1, *Yearbook of the International Law Commission* 2001, vol. II (Part Two), 144–170, 149–151; International Law Association, *Second Report on Due Diligence in International Law* (July 2016) 6. For cyber-specific applications, see Michael N Schmitt (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) 30–43; Karine Bannelier, 'Obligations de diligence dans le cyberspace: qui a peur de la cyber-diligence?' (2017) *Revue Belge de Droit International* 612.

their jurisdiction over ICT infrastructure within their territory',[83] seems to indirectly acknowledge its applicability in cyberspace. Often referred to as 'due diligence', the principle requires that States take appropriate measures to ensure that activities within their territory or under their jurisdiction do not cause significant harm to other States.

While the corresponding GGE norm is readily recognisable as a version of the due diligence principle, it presents a number of specificities. The norm reads as follows: 'States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs'.[84] The first observation concerns the choice of the word 'should'. Together with the introduction indicating that all the norms are voluntary and non-binding, the wording distinguishes this norm from the principle of due diligence, which, according to the International Court of Justice, is 'general and well-recognized'.[85] Another difference is contained in the term 'internationally wrongful acts', which denotes breaches of State obligations entailing international responsibility.[86] The general principle of due diligence is not similarly qualified but covers also private activities within the territory or jurisdiction of a State that cause or risk to cause significant harm to another State. In the area of international environmental law, the obligation to prevent transboundary harm to the environment of other States or areas beyond national jurisdiction often requires that States take legislative or other measures concerning private economic activity.[87] There is little reason to doubt the capability of non-State actors to cause harm in cyberspace, either. The 2013 GGE report acknowledges as much in stating that States 'should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs'.[88]

As formulated in the 2015 report, however, the relevant norm seems to address only State action, and more specifically cyber operations by States other than the territorial State. At the same time, it only covers situations in which the territorial State is aware of the wrongful action. Actual or presumptive knowledge is an essential element of the due diligence principle. Limited to situations in which the harmful activity constitutes an internationally wrongful act by another State, the conduct referred to in the norm – knowingly allowing the other State to use the State's territory – also comes close to assistance to a wrongful act. As such, it could be covered by the existing rules on aid or assistance in the commission of an internationally wrongful act.[89] While the norm can also be understood to extend to operations, in which harmful data is only routed through the territory of the State, it may be taken that the territorial State in such cases rarely has any knowledge of the on-going operation, or ability to take feasible measures to terminate it.

---

[83] GGE 2013 report (n 57) para 20.

[84] GGE 2015 report (n 3) para 13(c). For further discussion of due diligence in cyberspace see Antonopoulos (Chapter 6 of this Handbook).

[85] *Corfu Channel case* (n 81) 22.

[86] International Law Commission, Articles on State responsibility, art 1: 'Every internationally wrongful act of a State entails the international responsibility of that State', *Yearbook of the International Law Commission 2*001, vol. II (Part Two) 32–4.

[87] International Law Commission, Draft Articles on the Prevention of transboundary harm from hazardous activities (n 82) art 3 and commentary, 153–5.

[88] GGE 2013 report (n 57) para 23.

[89] International Law Commission, Articles on State responsibility (n 86) art 16 and commentary, 65–7. In general, however, a breach of the due diligence obligation may be easier to prove than aid or assistance, see Olivier Corten and Pierre Klein, 'The limits of complicity as a ground for responsibility. Lessons learned from the *Corfu Channel* case' in Karine Bannelier, Théodore Christakis and Sarah Heathcote (eds), *Impact of the Corfu Channel Case* (Taylor and Francis Group 2011).

It has been pointed out that non-binding, or 'soft law' regulations can in general be effective, provided that they meet certain conditions. For instance, non-binding regulations should be simple and clear,[90] and transparent in the sense of being recognisable as soft law.[91] What makes the norm at hand challenging in this regard is that it takes an existing legal norm as a template and uses specific international law terminology. Analysing and understanding the norm is only possible with reference to international law.[92] The ambiguity surrounding the norm with its strict legal drafting and voluntary nature may make it less successful in bringing predictability and stability to international relations.[93] At the same time, it may be taken to refer to the existing international law principle, which continues to require of States certain due diligence, including regarding cyber activities, in ensuring that no serious harm is caused to other States. A number of other norms in the 2015 GGE list can in this regard be seen as related to the general due diligence obligation, providing additional detail on how 'to ensure' that malicious or harmful cyber activities do not cause significant harm in another State. This would be the case, for instance, of norms regarding the protection of the critical infrastructure, the integrity of the supply chain, or prevention of the proliferation of malicious ICT tools and techniques.[94]

Similar kinds of questions related to international law are raised by the last remaining norm, according to which a State should not 'conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to public'.[95] The purpose of the words 'contrary to its obligations under international law' may be to carve out any lawful activity so described. This could be the case of situations in which self-defence or other circumstances precluding wrongfulness apply,[96] or of attacks during an armed conflict that may intentionally damage critical infrastructure, provided that such a target can be established as a military objective and the action fulfils other requirements of international humanitarian law.[97] As no explanation to this effect is given, the formulation of the norm also allows another and more question-begging reading, according to which it would be voluntary for a State to refrain from acting against its obligations under international law. The norm can further be taken to reaffirm that the obligations a State has in the kinetic realm also apply in cyberspace.[98]

---

90 Finnemore (n 26) 89, 91.

91 Christian Brünner and Georg Königsberger, 'Regulatory impact assessment' – a tool to strengthen soft law regulations' in Marboe (n 42) 95.

92 For a more elaborate analysis, see Liisi Adamson, 'Recommendation 13(c)' in Tikk (n 8).

93 GGE 2015 Report (n 3) para 9. See also Osula and Rõigas (n 28) 20.

94 GGE 2015 Report (n 3) paras 13(g) and 13(i).

95 Ibid., para 13(f).

96 International Law Commission, Articles on State Responsibility (n 86) arts 20–27 and commentary, pp 71–86.

97 See Schmitt (n 82) 401–511.

98 Jason Jolley, 'Recommendation 13(f)' in Tikk (n 8) 173.

5. RECEPTION OF THE GGE NORMS

The choice of norms as a method to regulate the area of cybersecurity is widely understood as an alternative to and a substitute for international law-making.[99] For some commentators, the preference for norms is a welcome way to avoid the rigidities of treaty processes,[100] for others a deplorable evasion by States of their responsibility as primary law-makers.[101] It has furthermore been submitted that the existing cyber norms could form 'an intermediate stage on the way towards the generation of cyber "hard law"'.[102] As pointed out above, non-binding articulations of normative commitments may perform different functions in relation to the development of international law. Regarding the GGE norms, attention should be paid, in addition to the questions of intent and content discussed above, to their reception by the broader community of States, the way in which they have been framed in the various statements of endorsement, as well as the follow-up given to them so far.

While most of the above-mentioned collective endorsements of the GGE norms stress the 'voluntary and non-binding' nature of the norms, they also contain calls for their effective and widespread implementation.[103] It is also worth noting that the norms proposed by the Global Commission on Stability in Cyberspace, as well as Paris Call principles largely cover the same questions as the GGE norms, thus reinforcing their core content while also complementing it with additional proposals. Various UN-led and regional programmes and workshops have promoted better understanding and implementation of the GGE norms.[104]

To a certain extent, however, the GGE norms may also have served as precursors for binding regulation at the regional level. This could be the case of the EU restrictive measures, which seek to deter and respond to cyber-attacks that have a significant effect and constitute an external threat to the Union or its member States. According to the relevant Council Decision, cyber-attacks constituting a threat to member States include those affecting critical infrastructure, services necessary for the maintenance of essential social or economic activities, including essential services to the general public, and government emergency response teams.[105] These elements of the relevant definition correspond to a number of GGE norms and have the force of law within the EU legal system. Another element referring to cyber-attacks that affect

---

[99] Finnemore and Hollis (n 2) 441.

[100] Joseph S Nye Jr., 'Eight norms for stability in cyberspace', *Project Syndicate* (19 December 2019) https://www.project-syndicate.org/commentary/eight-norms-for-stable-cyberspace-by-joseph-s-nye-2019-12?barrier=accesspaylog.

[101] Kubo Mačák, 'Is the international law of cyber security in crisis?' in Nikolaos. Pissanidis, Henry Rõigas and Matthijs Veenendaal (eds), *2018 8th International Conference on Cyber Conflict: Cyber Power* (CCDCOE Publications 2016).

[102] Kubo Mačák, 'From cyber norms to cyber rules: Re-engaging States as law-makers' (2017) 30 *Leiden Journal of International Law* 877, 894.

[103] E.g. the Lucca Declaration of G7, 3; Paris Call (n 6) Principle 9.

[104] See, e.g., UNIDIR and CSIS, *Report of the International Security Cyber Issues Workshop Series*, 2016, available at https://www.unidir.org/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf; 6 ARF (2015), ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies (7 May 2015) https://cil.nus.edu.sg/wp-content/uploads/2019/02/2015-ARF-WP-on-ICT-Security.pdf.

[105] Council Decision (CFSP) 2019/797 (17 May 2019) concerning restrictive measures against cyber-attacks threatening the Union or its Member States, art 1, paras 4(a), 4(b), and 4(e).

critical State functions, such as public elections or the voting process,[106] has a connection to some of the norms proposed by the Global Commission on Stability in Cyberspace and the Paris Call.[107]

The EU restrictive measures have also been described as 'a concrete mechanism to rectify the challenge of enforcement inherent to the voluntary and non-binding nature of norms in cyberspace'.[108] The Council Decision's link to the GGE norms is nevertheless only indirect, as the conduct that may trigger the imposition of sanctions is defined independently and not with an explicit reference to the norms of responsible State behaviour. At the same time, the EU cyber sanctions regime is indicative of a recent shift of emphasis from the implementation of the norms at the domestic level to compliance with them in international relations. The EU Cyber Diplomacy Toolbox, which preceded the restrictive measures, was motivated by the perceived need 'to clearly signal the consequences of malicious activities'.[109] The need for cyber deterrence was likewise recognised in the US National Cyber Strategy of 2018.[110] Reference can also be made to a statement by a group of States made in the UN General Assembly in 2019.[111] The statement described a 'framework of responsible State behaviour' consisting of international law and the GGE norms, and contained a commitment to work together 'to hold States accountable when they act contrary to this framework'.[112] The Global Commission on Stability in Cyberspace has as well recommended that States and non-State actors 'respond appropriately to norms violations, ensuring that those who violate norms face predictable and meaningful consequences'.[113] A number of recent attributions of harmful cyber operations to other States have furthermore highlighted the need for compliance with the norms of responsible State behaviour.[114]

It is notable that references to compliance, enforcement and consequences for conduct that violates the norms of responsible State behaviour in this context have not been articulated in terms of specific international law prohibitions, or conduct qualified as an internationally wrongful act. The responses, accordingly, have been limited to retorsions, such as statements, whether including an attribution or not, and restrictive measures. It is by no means unusual that expectations of compliance, monitoring, or sanctions are attached to non-binding norms.

---

[106] Ibid. art 1, para 4(c).

[107] GCSC, *Advancing Cyberstability* (n 5) Norm 2; Paris Call (n 6) Principle 3.

[108] Pawlak and Biersteker (n 22) 33.

[109] Cyber Diplomacy Toolbox (n 21). For the citation, see Paul Ivan, *Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox*. Discussion paper, European Policy Center (18 March 2019) 5.

[110] US National Cyber Strategy, September 2018, 21: 'United States will develop swift and transparent consequences […] to deter future bad behavior', available at https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[111] Joint Statement of Advancing Responsible State Behavior in Cyberspace, 27 States had signed in the statement in September 2019, available at https://nz.usembassy.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

[112] Ibid.

[113] GCSC, Advancing Cyberstability (n 5) Recommendation 2.

[114] Some of these statements also refer to international law, for an analysis see Giorgi Nakashidze, 'Cyberattack against Georgia and International Response: Emerging normative paradigm of "responsible state behavior in cyberspace"?' (28 February 2020) EJIL: *Talk!*, https://www.ejiltalk.org/cyberattack-against-georgia-and-international-response-emerging-normative-paradigm-of-responsible-state-behavior-in-cyberspace/.

At the same time, as Shelton has pointed out, adding law-like consequences to non-binding commitments is conducive to making the distinction between law and non-binding norms less clear.[115]

Consideration of the GGE norms from the point of view of the intent of the drafters, and their content, as well as further developments regarding their reception and impact suggests that norms are increasingly accorded an independent role in defining and regulating 'responsible State behaviour'. At the same time, the relationship of the norms with international law is in some respects strained. It remains to be seen how much the various UN groups with a cybersecurity agenda will invest in norms discussion, adding clarity to where there is ambiguity or room for confusion, or developing new norms, possibly inspired by the Global Commission on Stability in Cyberspace, the Paris Call, or other such initiatives. Development of binding treaty obligations, while not excluded as an option, would be conditioned by the very real disagreements that have been evident in the UN discussions in recent years. This, too, adds value to the cyber norms as a common point of reference.

[115] Shelton (n 25).

3. Mapping power in cyberspace

Outi Korhonen and Ekaterina Markovich[1]

1. INTRODUCTION

The discourses about cyberspace and, in particular, its regulation or, more broadly, its governance are discourses of power. Yet, most of the cyberspace-related power and distributional questions seem obscured if not wholly unknown to us. Both good and bad effects produced by emerging digital technologies appear as 'the unintended variety, as society grapples to adapt to technological change it does not fully understand'.[2] It is well known that 'power is most effective when least observable'.[3]

We seem to identify certain debates, such as those concerning privacy, surveillance, cyberterrorism and security in which we engage vigorously but episodically. The general audiences do not possess or even seek a holistic view of cyberspace governance architectures or the ideological stakes in the struggles that take place in our virtual environment. Meaningful interventions into cyberspace power distribution are, however, impossible through piecemeal engagements, whose situatedness in their richer contexts escapes us. In order to weigh in the debates one must have some idea of who owns, who controls and who designs and shapes cyberspace with what kind of tools. This is of fundamental importance, since power can be defined as 'the force to bring about – or to prevent – social, political, or economic changes'.[4] Power is so multiple that change or its prevention does not have to take place by physical force or overt subordination; it can also result from the exercise of slow violence,[5] epistemic violence,[6] systemic or structural violence[7] or coercion in the everyday rather than at the celebrated summit meetings. To debate about distributional matters in cyberspace does not make sense unless we identify subjects and objects, the 'whos', the 'whats', the 'hows' and 'the what withs'. Only upon such knowledge can we intelligibly ask how we can intervene and participate in change-making and how international legal tools may be operationalised to support better distribution globally. While the economy and governments become ever further digitalised, most of the distributional stakes cannot be assessed or accessed with the tools and know-how of the IRL-world (the in-real-life world). At present we may lay our hopes with, as Lawrence Lessig puts it, the culture of the code and the coders[8] i.e., we must contend to

[1] The chapter was written with the assistance of Henrik Jylhä-Vuorio and Saara Monthan**.** All websites were last accessed on 13 November 2020.

[2] Alan Z Rozenshtein, 'Wicked Crypto' (2019) 9 *UC Irvine Law Review* 1181, 1182.

[3] Steven Lukes, *Power: A Radical View* (Palgrave Macmillan 2004).

[4] Kenneth Clarke, *Dark Ghetto: Dilemmas in Social Power* (Harper & Row 1965) 199.

[5] Rob Nixon, *Slow Violence and the Environmentalism of the Poor* (Harvard University Press 2011).

[6] Kristie Dotson, 'Tracking Epistemic Violence, Tracking Practices of Silencing' (2011) 26 *Hypatia* 238, 236–7.

[7] Johan Galtung, 'Violence, Peace, and Peace Research' (1969) 6 *Journal of Peace Research* 167.

[8] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999) *passim*.

be happy to leave it all (designs and decisions) for the experts to rule through their everyday activities. Yet, coders and their culture is even less familiar than that of the proverbial faceless bureaucracy, whose role the invisible coders are emulating in cyberspace.

The code and the so-called algorithmic governance derived from self-executing coded procedures is certain to increase formalism – in which human interference and discretion is seen as suspect meddling, even arbitrariness, opening the doors for unequal treatment, corruption and subjective bias. Also, the coding industry wisdom is that only very few of the vast armies of coders (technical programmers) come up with their own solutions rather than copy-paste existing pieces of code from open and non-open sources. However, the only debate seems to be about whether copyright is widely infringed by the industry and the fact that only the small minority writing their own code and thus thinking through the different layers of their programming solutions will stop to give any thought to the political and ideological stakes that are embedded in e.g., standardised pieces of smart contracts or the like.[9] Furthermore, the extreme formalisation that coding gives e.g., to a contract, derives from the nature of the coding and its axiomatic technological formalism. In coding, human expression is pulled through the sieve of qualitative language theory that strips away all leeway, discretion and ambiguity while it reduces expressions to sequences of zeros and ones, thus creating precision through reduction and formalisation.[10] Rather than a culture of formalism, as Martti Koskenniemi's international lawyers imagined good governance,[11] we might be entering an era of the un-culture of ultra-formalism and reductionism.[12]

The institutions, operations and global designs of and for cyberspace are, for the most part, very poorly known. Most cyberspace users cannot name the organisation that manages and controls internet domain names nor can they explain the infrastructure that maintains the cyberspace or its owners. Whether these actors have any power over our digital life, whether they have any principles or visions for cyberspace, is mostly not known and not discussed even when we debate, say, a particular bill's effect on privacy or other basic rights. Indeed, we know not under what kind of international agreements the bits pass in the sub-ocean cable networks or filter into our homes from telecom towers and through optical fibres. Most of us have been astonished to suddenly wake up to the fact that there is a new power centre in the world called GAFA (Google, Amazon, Facebook and Apple) or Big Tech, which, allegedly, can have presidents elected and death penalties executed. They control at least '55% of our digital life' and hold well over a hundred billion dollars in accessible cash reserves.[13] Yet, these anecdotal facts are but a drop in the ocean that would make global cyberspace familiar to its users. It seems as if many of us are resigned to wandering in a dark jungle without a map, raising disproportionate alarms when we think we hear a threatening predator nearing; never

---

[9] See https://www.zdnet.com/article/are-developers-stealing-code/.

[10] See Philip Agre, 'Toward a Critical Technical Practice, Lessons Learned in Trying to Reform AI' in Geoffrey Bowker, Les Gasser, Leigh Star and Bill Turner (eds), *Social Science, Technical Systems, and Cooperative Work: Bridging the Great Divide* (Erlbaum 1997).

[11] Martti Koskenniemi, *The Gentle Civilizer of Nations: The Rise and Fall of International Law 1870–1960* (CUP 2001) 500.

[12] This caution has been urged by David Kennedy during many seminar discussions attended by the authors.

[13] Pierre Maurin, 'Google, Amazon, Facebook and Apple, a New Economic and Managerial Model', *Alhambra* (13 July 2015) https://www.alhambra-international.com/google-amazon-facebook-and-apple-a-new-economic-and-managerial-model/.

knowing for certain whether it is real or a myth, not being able to situate it within the reference field of our life-world or political economy.

Senior legal and governance experts openly admit not recognising the vocabulary of cyberspace or social media (SOME) from pods to tweets or digital currencies to cryptos, yet they are daily called upon to advise on their normative governance. The roles of ISOC, IAB, IETF, IASA, IESG and ICANN[14] are minimally known and their power mystified in ways that the WTOs, the WEFs, the World Banks or the IMFs in the global political economy never were despite the harsh criticisms directed toward the role of the latter in preventing any new international economic order initiatives from launching. Whilst the role of the former is different, they nevertheless are loci for concentrations of power that shape cyberspace and through it transform or prevent change in our lives.

This chapter calls for demystification of power in cyberspace – or cyberjungle, as it seems at present. It is impossible to identify actors, their visions, openings for engagement and empowerment if we approach cyberspace discourse as latter day Latin, as yet another technocratic expert language. This chapter also takes a contrary view to cyber realism – a theory about the possibility and desirability to govern cyberspace similarly to any territory or physical object through analogising cyber phenomena to IRL-phenomena and tracing cyberoperations back to physical territories through the IT-hardware.[15] While such an approach is needed in many instances, it invites intellectual resignation in the face of a space in which different kinds of architectures, designs, interactions, identities and border-drawings emerge. To assert that it can be tied down to physical equivalents is proving impossible e.g., in the debates on taxation of international digital business[16] threatening to extend to a digital tax war.[17] Only through demystification and learning about cyberspace architecture, its various architects, their grammar and tools can we avoid uninformed fear-reactions or frustrated resignation.[18] It seems a question of personality whether we see 'cyberstuff' – from cyberspace to cybercrime, cyberwar to crypto assets – as fearsome threats and challenges to social order; or, in the other extreme, as an exciting wilderness of positive challenges that invite us to reinvent organising 'otherwise'. Without studying the dynamics, modes, structures and sources of power in cyberspace, we forgo any chance to participate in creating positive change through the digital dimension of our world.

---

[14] These are organisations, which provide inputs to the ecosystem of cyberspace by e.g., dealing with open standards and operational issues of the Internet and also by managing the Internet's infrastructure. In a way, they oversee cyberspace; see Darrel Ince (ed), *Internet Society, A Dictionary of the Internet* (OUP 2019).

[15] See in this regard Tsagourias (Ch 1 of this Handbook) and Kohl (Ch 4 of this Handbook).

[16] Marcel Olbert and Christoph Spengel, 'International Taxation in the Digital Economy: Challenge Accepted' (2017) 9 *World Tax Journal* 3.

[17] See Alan Rappeport,Ana Swanson,Jim Tankersley andLiz Alderman, 'U.S. Withdraws From Global Digital Tax Talks', *New York Times* (17 June 2020, Updated 12 October 2020) https://www.nytimes.com/2020/06/17/us/politics/us-digital-tax-talks.html.

[18] David Kennedy, *A World of Struggle: How Power, Law, and Expertise Shape Global Political Economy* (Princeton University Press 2016) 5, 172.

2. CYBERSPACE SUBJECTS, OBJECTS AND TERRAIN

The legal subjects of cyberspace are mostly international legal subjects. The vastly powerful transnational private actor ICANN has an explicit duty to operate under international law.[19] Private organisations, such as corporations or associations, tend to have transnational ownership, participants, clients, goals, or all of them. States and international public organisations, have long since embraced cyberspace activities; other examples include Estonia's e-government,[20] the EU's cyber policies;[21] the United Nations' many cyber working groups;[22] Georgia's crypto farms;[23] the cyber security and cyber war capabilities of the North Atlantic Treaty Organisation;[24] and many States[25] etc.

Also, the 'space' of the cyber-world, where all the action takes place, is more a question than a given. Is there a separate cyber territory or is the cyber activity – for the purposes of its normative governance – reducible to State territories and international areas corresponding to their international doctrinal criteria? Or, is it a hybrid of the two, partly *sui generis* partly reducible to the doctrines governing territorial acquisition, control, ownership, accession, secession, status as commons/common heritage, dominion, jurisdiction etc?[26] The more obscure its design and the more tied back to the existing institutions, the less the chances

---

[19] Mark Leiser and Andrew Murray, 'The Role of Non-State Actors and Institutions in the Governance of New and Emerging Technologies' in Roger Brownsword, Eloise Scottford and Karen Yeung (eds), *The Oxford Handbook of Law, Technology and Regulation* (OUP 2017).

[20] To demonstrate, in Estonia's digital society, 99 per cent of public services are online, 44 per cent of participating voters used internet voting to elect their government and the number of e-Residents is already approximately 66, 000. For more information see https://e-estonia.com/.

[21] On 27 May 2020, the Commission adopted a new communication; *Europe's Moment: Repair and Prepare for the Next Generation* (27 May 2020) https://ec.europa.eu/commission/presscorner/detail/en/ip_20_940. As a part of the package, the new Cybersecurity Strategy will look at how to boost EU-level cooperation, knowledge and capacity. For more information on the EU cybersecurity strategy see https://ec.europa.eu/digital-single-market/en/cyber-security. See also Wessel (Ch 23 of this Handbook).

[22] For instance, the UN Group of Governmental Experts (GGE) aims to establish norms, rules and principles for States and responsible conduct in the realm of cyberspace; see https://www.un.org/disarmament/group-of-governmental-experts/. The UN Open-Ended Working Group (OEWG) is set to proceed developing these rules, discuss their further application and to enhance subject related dialogue within the UN; see https://www.un.org/disarmament/open-ended-working-group/. For the UN's approach to cyber security see also Henderson (Ch 28 of this Handbook).

[23] In 2017 Georgia was the second largest cryptocurrency miner in the world – having only China ahead of it. For global cryptocurrency mining map, see Michel Rauchs and Garrick Hileman, 'Global Cryptocurrency Benchmarking Study' (Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School, 2017) https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/global-cryptocurrency/#.X43X1O0o9PY.

[24] NATO's policy on cyber defence brings forth how maintaining strong cyber defence is one of the core tasks of the Alliance's collective defence. See
https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf. See also Hill (Ch 24 of this Handbook).

[25] For instance, all EU member States had issued national cyber security strategies by 2017. For more information on such strategies, see the ENISA NCSS Interactive Map;
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

[26] See Tsagourias (Ch 1 of this Handbook), Lehto (Ch 2 of this Handbook) and Kohl (Ch 4 of this Handbook).

of radical reimagination of institutions and partnerships. It seems that the existing positions of digital realism and cyberspace as *sui generis* are often based more on preference than critical analysis. We might accept or even applaud the constant rising of the level of legal specialisation and expertise in doctrinal intricacy and, hence, advocate for highly specialised cyberspace law; or we might root for a Lauterpachtian sensibility in that we like to think of lawyers capable of governing and advising on the basis of analogical reasoning even in case of *lacunae* in law.[27] The present chapter proceeds from the hypothesis that both of these positions are lacking. Cyberspace agency, regular and legal personalities, presence, occupation, dominion, action, institutions, and responsibilities sometimes do and sometimes do not utilise, correspond or call into question international legal categories.

3. ENCRYPTION AS BASIS OF CYBER CULTURE

In order to ground our emerging sketches of cyberspace and its power dynamics, we have to know about the building blocks, tools and ingredients that affect distributional gains in cyberspace. Encryption, in technical terms, is a means of scrambling data to protect private information and communications; in social terms, it founds the culture of cyberspace and of the 'internet society'. Encryption is achieved through code and is studied by the discipline of cryptography. The proper or permissible amount of encryption is a long-standing debate that, in parts, invokes similar cultural concerns as the Islamic veil ban cases in which European governments have successfully asserted that too much veiling risks public order and violates the 'space of socialization' necessary for living together.[28] A total absence of encryption, in the other extreme, would be greatly more disturbing and risky to public order than nudity. Encryption acts as our skin in all of our life that we live in cyberspace, yet most do not even recognise the concept. In practice, it is the commercial services – Amazon, Facebook etc. – who give this 'skin' to us when we use their platforms. Since most are not familiar or interested in what kind of skin these commercial actors provide for us, they often retain the ability to get under our skin; the Cambridge Analytica scandals exposed how Facebook profiles and sells the intimate details of its users' lives and identities. Yet, the power of Facebook and the other cyberspace giants proved resilient to any change that IRL-governance institutions, including US courts, attempted to demand of it.[29] Although there has been a significant exodus from Facebook accounts by users whose intimate information and images had been sold and exploited, the company has diversified its empire and developed a dependency among its digital platforms so that it stays part of people's digital lives regardless of whether they continue to have a Facebook account.[30]

---

[27] Hersch Lauterpacht, *The Function of Law in the International Community* (OUP 1933).

[28] Sital Kalantry and Maithili Pradhan, 'Veil Bans in the European Court of Human Rights' (2017) 21 *ASIL Insights*, https://www.asil.org/insights/volume/21/issue/15/veil-bans-european-court-human-rights.

[29] Julia Carrie Wong, 'The Cambridge Analytica Scandal Changed the World- But It Didn't Change Facebook', *The Guardian* (18 March 2019) https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook.

[30] See Mark Scott, 'Facebook's Digital Empire Hard to Shake Despite Cambridge Analytica Scandal', *Politico Pro* (25 March 2018) https://www.politico.eu/article/facebook-cambridge-analytica-mark-zuckerberg-data-protection-privacy-instagram-whatsapp-deletefacebook/.

If we want to take control of our identity-protecting 'skin' in cyberspace and stop the mindless hitting of the 'consent' icons on every digital service that we use, we should understand the basic logic. Encryption comes in many modes: symmetric, asymmetric, one-end, end-to-end, link, elliptic, data-at-rest;[31] and it comes on many levels of strength, with or without digital key escrows or backdoors, in-built weaknesses, and recovery options. The military and hard security circles are the homebase of strong encryption in which it is developed and advocated. The American military research funding is the main driver of encryption as most other digital technologies and innovations, such as artificial intelligence (AI). The needs of the military are the prime concerns while, at the other end, we intuitively fear that the distribution of strong encryption capability may boost the gravest forms of international criminality – and its ability to 'go dark'. The discourse of strong encryption and hard security is well-known from e.g., NATO.

Encryption technology is the cultural grammar of cyberspace. It is crucial in determining the social conditions and the culture of the digital realm. By encrypting their personal and other data, individuals and communities define their digital identities, their interfaces, contact channels and expression of e.g., trust. Encryption enables the exclusion of others' interference into one's digital private sphere, the exposure, the secrecy of digital correspondence, and the gatekeeping by digital communities unless, as is mostly the case, one delegates the provision and maintenance of this essential 'skin' to a party such as Facebook. Oftentimes, public interest requires information, transparency and participation from society members. Hence arises the need for decryption and opening of bounded spheres. There is no full and permanent solution to the question of whether public authorities should always have spare keys and backdoors for every sphere in case of emergency needs or lesser yet legitimate public purposes. Encryption will always enable some exclusion, provide tools for hiding, covering and enable measures of extreme distrust; in this respect, it does not differ from physical reality. In the traditional sense, one can also clothe, veil, disguise, disappear, hide, build walls, erect barbwires, become a recluse or drop off the grid; furthermore, there is no way to prevent the use of either traditional or digital currencies for crime. Similarly to encryption technology, there is no full answer or absolute solution. The level of encryption and who is allowed to exercise it creates a mood in the digital environment that makes it more or less like a railway station (open, public) or a rented flat (walled). In the latter, the superintendent has the master key and emergency personnel can break in if need be. Encryption carves up exclusive 'spaces' and lines of communication and its strength defines whether and when access is possible.

In the encryption discussion, alarmism, storms, utopias and dystopias are common. They flag the power struggles even if only on the surface. Threatening notions are designed to scare the public for quick political gains; we are told that we must avoid, at almost any cost, the 'going dark of the bad actors'; whereas on the opposite (libertarian) side, we are warned of the 'golden age of surveillance' and the even bigger digital Big Brother.[32] The expert discourses identify 'crypto wars'. Few know what is at stake but stereotyped positions, such as

[31] There are different ways of ensuring information safety. They vary e.g., in the number of cryptographic keys used to achieve encryption and therefore serve different purposes.

[32] See e.g., James B Comey, 'Going Dark: Encryption, Technology and the Balances Between Public Safety and Privacy', *Federal Bureau of Investigation* (8 July 2015) https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy; Peter Swire, 'The Golden Age of Surveillance', *SLATE* (15 July 2015).

'China spies' or 'no more government', are drummed up to support policy solutions that stem from garden variety geopolitics of fear,[33] libertarian dreams[34] or simple preferences such as uncritical techno-positivity or techno-adversity. This superficial power discourse often misses the point, is spotty, isolated, episodic and understood as separate from the ethics of emerging technology. The nuts and bolts, cables, valves and switches, soft and hardware, infrastructure and electric-grid provision, the contracts and property entitlements, on which digital services rest, stay effaced from the discourse as do the institutions and architects. Even the advocates of digital realism pay little or no attention to the ownership and property-derived power embedded in the hardware, its owners, its maintenance and its operators while, otherwise, advocating the analogising of digital phenomena to those of the 'real' world.

A report drafted by the NATO Parliamentary Assembly in 2018 expresses how encryption discourse remains in the centre of attention due to the disruptive technology's possibility to impact on policy issues regarding security.[35] The report argues that instant messaging services providing strong encryption such as Telegram are being used by terrorist groups to command and control. As such, technologies provide terrorists with new means and methods to act; the report suggests that 'robust policing of and strong regulations for cryptographic technologies are necessary'. The report however acknowledges also the difficulties in balancing between fundamental rights and security concerns. As the problematic side of modern encryption unveils, the discourse starts portraying robust desires of keeping strong encryption out of the hands of malicious actors. Examples vary from banning exports of strong encryption technologies[36] to demands of government 'backdoor-access' to instant messaging services in pursuit of protecting the public from acts of terror.[37]

Export restrictions on encryption technologies tend to fall under arms export control regulations; this is an important point to remember together with the fact that the same technology is the identity-creator/protector of the individual and the emerging modes of activism, cooperation and partnerships. Encryption technology export controls are high on international or national sanction and trade embargo lists e.g., set against North Korea, Russia, China, Iran and Venezuela by the West.[38] They predict the risks caused by 'bad men' and aim to protect

---

https://slate.com/technology/2015/07/encryption-back-doors-arent-necessary-were-already-in-a-golden-age-of-surveillance.html. On cyber espionage see Buchan and Navarrete (Ch 11 of this Handbook).

[33] Rachel Pain, 'The New Geopolitics of Fear' (2010) 4 *Geography Compass* 226.

[34] Primavera de Filippi, 'Bitcoin: A Regulatory Nightmare to a Libertarian Dream' (2014) 3 *Internet Policy Review*, https://policyreview.info/articles/analysis/bitcoin-regulatory-nightmare-libertarian-dream.

[35] NATO, *Science and Technology Committee, Sub-Committee on Technology Trends and Security, Dark Dealings: How Terrorists Use Encrypted Messaging, the Dark Web and Cryptocurrencies* (2018) https://www.nato-pa.int/document/2018-dark-dealings-tonin-report-182-stctts-18-e-fin.

[36] Ben Buchanan, 'Cryptography and Sovereignty' (2016) 56 *Survival* 95.

[37] See https://www.forbes.com/sites/nikitamalik/2018/11/07/the-tradeoff-between-security-and-privacy-how-do-terrorists-use-encryption/#107e627a62d8.

[38] For instance, the US Department of Commerce, Bureau of Industry and Security issued new rules in April 2020 that resulted in expansion of military end use and end user control on China, Russia and Venezuela. In other words, greater export restrictions hit a broad spectrum of encryption based commercial items on these countries. See more at https://www.govinfo.gov/content/pkg/FR-2020-04-28/pdf/2020-07241.pdf.

international and/or national security and law enforcement.[39] The bad man of the digital age comes in various guises from rogue regimes to drug lords, child pornographers and sex traffickers to name the most commonly invoked *hostis humani generis* in this context. They are among the most feared actors of cyberspace; those subjects whose repression is often the main goal and motivation of any cyber policy i.e., they are gauged as cyberterrorists.[40] With these labels, people are warned against everything 'unknown' and, thus, everything radically new and unfamiliar emerging in cyberspace. Alongside the military, the centres of financial power are a main driver of the development of cybercommerce, trade and operations that require strong encryption. They need the most robust strongholds and dominate the digital landscape. Their dominating presence and available funding make them architects of cyberspace culture. They claim to need a thick digital skin or, better expressed, a veritable fortress, and no one seems to question it. In the West, favourable treatment is granted to the encryption needs of financial institutions, insurance and medical business purposes, and online merchants in that order, while we are suspicious of its global proliferation. As a logical consequence, although rarely explicitly recognised, such preferential trade policies operate to widen the digital divide between the North and South and, on the other hand, the cleft between global financial centres, mega companies and regular-size or tiny businesses. The 'cyber-needs' of global finance are taken as givens; and regulators cater to their normative requirements without questioning the impact on global financial and digital peripheries. Again, the individual, a 'rogue State' or the small organisation is often not allowed such a 'skin' – i.e., the strong encryption technology – because of the fear that it might harbour bad men or lure them into the 'dark web'. The architecture of cyberspace dominated by the fortified military, financial, Big Pharma and online merchant institutions would raise attention if it was built in the physical world and we could perceive the taunting disproportion between them and other actors. However, before we learn to see into cyberspace we do not pay attention to how it is constructed and dominated, as happened with the growth spurt of the GAFA.

Apart from the Global South, internet proponents, privacy and free speech activists and many commercial actors demand lesser restrictions on encryption and cryptography. The United States, the world leader of encryption knowhow followed by Israel, Germany and the United Kingdom (the world leading military industry States), has periodically eased trade restrictions in exchange for increased demands of international regulation, extraterritorial jurisdiction, disclosure of buyers/users' personal data.[41] However, contemporarily, the US has kicked up 'a perfect storm' that seems to blow ever further away any hopes of international or even transatlantic agreement on sanctions,[42] including those concerning the defence and intelligence sensitive encryption items. Moreover, the Trump administration has taken issue with Chinese SOME-companies WeChat and TikTok trying to first force a Microsoft acquisition of the latter with extraordinary cash proceeds to the government, and then abandoning it for another business stratagem. The federal government initially issued a conditional ban of

---

[39] Oliver Wendell Holmes Jr, 'The Path of the Law' (1897) 10 *Harv. L. Rev*. 457, 459.

[40] See Ileana Porras, 'On Terrorism: Reflections on Violence and the Outlaw' (1994) *Utah L. Rev*. 119.

[41] See e.g., Rändi Bessette and Virginia Haufler, 'Against All Odds: Why There Is No International Information Regime' (2001) 2 *Int'l Stud. Perspectives* 69.

[42] Ville Sinkkonen, 'Sanctions and the US Foreign Policy in the Trump Era, A Perfect Storm', *FIIA Briefing Paper* (2019) 269, https://www.fiia.fi/julkaisu/sanctions-and-us-foreign-policy-in-the-trump-era-a-perfect-storm.

TikTok's service and gave Microsoft time to proceed with acquisition and supervised the deal because of 'concerns that the Chinese-owned video app could pose a national security threat by funnelling personal information about United States citizens to the Chinese government'. *The New York Times* quoted President Trump saying: 'This data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information — potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage.'[43] And, while we watched the Trump performance, we ignored the size and economic stakes of the forced acquisition. After, however, these plans fell through, the Trump administration followed up with the threatened sanction; as of September (2020), WeChat and TikTok were banned in the US by the Department of Commerce that justified the action by claiming that both of the services were 'active participant(s) in China's civil-military fusion and (...) subject to mandatory cooperation with the intelligence services of the CCP (Chinese Communist Party)'.[44]

3.1 Encryption as Core of Digital Freedoms

For a libertarian, encryption is the integrity and authenticity, even dignity, device of the digital environment in which a person's data and digital identity is not otherwise protected by physical walls, surfaces or skins of any kind. The digital environment does away with our familiar face-to-face meeting, physical territory and borders. It also disrupts our familiar physical reality-based ideas of movement, storage, and archiving, which may be analogised but not reduced back to legal concepts developed for the physical realm. Although digital realism maintains that analogical application of existing governance technologies will be able to manage the digital economy and reality at large, oftentimes the analogies are clumsy if not violent when trying to fit the glass shoe of the physical-reality legislation on the foot of the virtual-reality phenomenon e.g., when governance agencies struggle with the question of whether posting cryptographical ideas on one's personal internet page is 'export' or not.[45]

To balance the public security interest to keep checks on the terrorist, criminal and other bad actors and the private interest of liberty (integrity, privacy, speech, association), encryption regulations have set conditions for the free sale, publication, communication, export and development of cryptographical items. These include e.g., prior public agency review; disclosure of recipient identities; limits on the strength of the encryption made available; favourable treatment for domestic and favoured nations markets; release only after similar technological advances become also available from elsewhere; and prohibition lists excluding terrorist supporters, military use-products and very strong items from free distribution. Also, the distribution of encryption source code is usually regarded as less risky than functional items while source code is understood as theory or ideas rather than readily workable practical tools.

---

[43] Michael D Shear, Alan Rappeport and Ana Swanson, 'Trump Wants US to Get Cut of Any TikTok Deal. No One Knows How That'd Work', *New York Times* (8 August 2020) https://www.nytimes.com/2020/08/08/us/politics/trump-tiktok-deal-treasury.html.

[44] See US Department of Commerce Press Release (18 September 2020) https://www.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect.

[45] Cindy Crohn and Andrew Crocker, *US Export Controls and Published Encryption Source Code Explained* (2019) https://www.eff.org/deeplinks/2019/08/us-export-controls-and-published-encryption-source-code-explained.

Absent from the language of private organisations seems to be the discourse on the need to develop the doctrines of digital commons, technology transfer, equitable sharing, compulsory licensing or co-dominion.

Because encryption is both a very lucrative global industry – providing skins, communication channels, social platforms, and distinguishable voices for all new sorts of animals spurning on the internet – and cryptography is one of the quickest developing academic fields, public actors reserve the strongest restrictions to fight against terrorism, organised crime, manufacture of weapons of mass destruction and the sexual exploitation of minors. The category of harmfulness to (inter)national security is criticised for vagueness; it is seen as boundless to the point of granting the public authorities absolute discretion and, therefore, strongly opposed by many interest groups – both for the public and for business. The so-called ICT-community (information and communication technology community), e.g., the pro-internet actors, such as *The Internet Society*, represent a large stakeholder community from companies to academics.[46] On the EU Council-level, topics such as internet governance, information and communication technologies are handled by the Working Party on Telecommunications and Information Society. They issue press releases and draft policy proposals for the United Nations, the G-20 and other fora to advance their interests in the governance of the encryption-related wicked problems.

3.2 Confused 'Thirty Years War'

The height of the stakes in the debate about creating digital skins, delimitations and thus spheres of self-determination and autonomy in cyberspace is demonstrated through the finger-pointing rhetoric. The stormy Trump deals and coercions aside, one of the main debates, the so-called *Crypto Wars* has raged in the mode of a Thirty Years' War between the (inter)national security demands for surveillance and decrypting possibilities and the ICT-community arguing for individual liberties and freedom of commerce. Yet, as in the Thirty Years War, many struggles and battles are fought under the media or at least the general public's radar. More recently, since international economic competition is a major driver for governments, many Western States have retreated from their deepest trenches except for the periodic resurging of the inter/national security alarms, such as with 'the war on' or 'fight against terrorism'. They have resurfaced in familiar terms in the debates concerning the risks associated with the cryptocurrencies, and, lately, the Trumpian geoeconomics leading to the 'perfect sanctions storm'[47] and forced acquisition deals. Interestingly, Crypto Wars corresponds very much to what David Parrot argues about the Thirty Years War which 'was a series of conflicts that merged together rather than a single war… [and] reflected different, albeit interconnected, sets of aims and security concerns'.[48] The nature of Crypto Wars is in many ways alike: its lifeline

---

[46] For ICT-community initiatives see e.g., Joint Call to World Leaders for A Healthy Digital Society, https://g20openletter.org.

[47] See Sinkkonen (n 42); Karen Lowell, 'Civil Liberty or National Security: The Battle over iPhone Encryption' (2017) 33 *Ga. St. U. L. Rev*. 485; Eric Manpearl, 'Preventing Going Dark: A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate' (2017) 28 *U. Fla. J. L. & Pub. Pol'y* 65, 68–76.

[48] David Parrot, 'The Thirty Years War, 1618–48' in John Andreas Olsen and Colin S Gray (eds), *The Practice of Strategy: From Alexander the Great to the Present* (Oxford University Press, 2011) 132–54.

is composed of separate events that gain impetus from different but interwoven multifaceted societal struggles that take unfamiliar modes while they also concern or are caused by emerging or imagined subjects, objects and possibilities in cyberspace. And, the general public in the involved countries have little if any knowledge why and over what the struggles are.

4. INTO THE UNKNOWN: USE OF THREATS AND MYTHS AS POWER

Remembering Bruno Latour's *We Have Never Been Modern (1993)* and his question if railway is local or global,[49] we can ask what is cyberspace? Is it global, is it local? Who controls its parts, is there any entity that has a clear view over the whole road? There are various ways to answer these questions and each answer may potentially result in a sharp turn in legislation, be it in the direction of restrictions, freedoms or a new melange. The problem is, however, that there are too many myths that hinder both lawmakers and the general public from recognising the gaps, conflicts and ambiguities in the available information and in the public debates. The familiar alarmism about loss of privacy or increased surveillance occasionally flares but it remains abstracted when we cannot situate these stakes in the grander design or even in our life-world virtual or real. The sheer complexity and the pace of the SOME-world (or Internet 2.0) do not invite its dwellers and users to in-depth reflection while they provide the constantly updating surface of distraction that crowds all perception and people's spare time. Instead of dwelling, cyberspace invites continuous surfing.

Cyberspace is often viewed as something that is not at all distant to the real life dimension in which our physical bodies exist, and in which borders can be marked by building a wall; in which money is something that one can hold in our hands, and communication is conducted face to face. The opposite view emphasises that cyberspace is unknown territory that has nothing to do with reality, classical borders, laws, means of communication or trade. The more sober view would proceed from the intertwining of these very different spaces that create very different conditions for being human today. Yet, we cannot examine these different but merged conditions if our imaginations are full of scary monsters like 'algorithms', 'encryption', 'bitcoin', 'blockchain', 'profiling' and others, ruled by The Anonymous who holds the power from which we can only feel increasingly alienated. The extremist yet commonplace views produce more questions than answers, more fears than logic, and hence the responses that we see all around the globe; they tend to be reactive, restrictive and invasive: 'If unsure, issue complete ban', which always tilts the balance in favour of stabilisation. And thus the power exercised by the 'real' world lawgivers acts to freeze transformation and prevent change through the openings created by the conditions of life in cyberspace. Our discourse is dominated by security rhetoric in which conflicts of rights are used as legitimate justifications to introduce mass surveillance or citizen profiling, similarly as they are used to justify targeted killings. Whenever a new 'danger' arises, there is arguably a pressing need to indiscriminately limit freedoms, rights and privacy as we have seen during the Covid-19 pandemic response. However, those who knew their way around cyberspace grew and profited immensely while those quarantined in their homes and focused on the familiar world of lost jobs and opportu-

[49] Bruno Latour, *We Have Never Been Modern* (translated by Catherine Porter, Harvard University Press 1993) 117.

nity: 'The Nasdaq (...) hit record highs during the pandemic, while the Dow Jones Industrial Index has not recovered its COVID-19 losses', reported The Forbes.[50]

The rapid evolvement of technologies during the past decades has been widely discussed as well as the changes that the growth of the internet represents for our daily lives. There are enormous quantities of data flowing around in cyberspace – that are available for grabbing, known as 'data mining' and often characterised as the 'oil' of the new millennium. Naturally even more has been said about the dangers presented by them. The impact of technologies on individual rights has long been of concern for the lawmakers, corporations and human rights defenders. Efforts to regulate this impact, improve transparency and set safeguards have been introduced by many States,[51] at least on paper. Yet there are uncertainties, fears and a growing number of myths about cyberspace that mark the general discourse. We do not realise that traditional means of protection have very limited power in cyber relations and thus the internet-using person while online can be easily stripped of any protection that, in the familiar 'real' world, was provided through national borders, geographical location and individual identity. Some contend pessimistically that the internet brings about a disembodiment that leads, in turn, to the absence of presence and therefore the absence of power. In terms of the encryption discussed above, one can easily and without even knowing it, let and even authorise various actors to peek and even reach inside one's digital skin – and thus penetrate and even destroy any legally mandated data protection. The variety of sad stories of the teenagers whose 'nude pics' circle in the social media for eternity represent an example of an utter loss of power and an eternal humiliation. In a further dimension, individuals interact in a reduced State of anonymous objects, disaggregated objects, which results in angst and susceptibility to fearmongering through security discourse. A 'tight', independently managed encryption skin is available only to the tech-savvy, the experts or the big actors such as banks, insurance, security and military actors, whose structures and funding dominate the present and future cyberspace visions.

Public anger is often directed at the corporations that collect vast quantities of user data in order to exploit and abuse it in many unknown and even unknowable ways while the data trickles down in digital value chains and is often under the control of no one or too many corporations for anyone to keep track. Myths are being blurred with facts, deliberately or unknowingly. Heated debates take place globally as soon as news of another data breach or loss is made public. In these debates, besides 'evil corporations', the other sort of entity that collects and exploits data is the State itself. As the world progresses ever further and deeper into the age of information, the lives of all are affected. Individuals are being actively profiled every minute, behavioural choices, locations, purchases and other information are being monitored, stored, analysed and nudged by the States in the very same manner as by advertising agencies, social media, other commercial and non-commercial entities – and definitely not only by the CCP. If we seek information on hammers on the internet, we are almost instantly bombarded with adverts of hardware because our desire has not only been 'seen' but also recorded and forwarded by the panopticon to circulate around the web for eternity. As ever more States

---

[50] Rachel Pupazzoni, 'Tech Stock Bubble Warnings Rise Amid Coronavirus Rally', *The Forbes* (14 July 2020) https://www.abc.net.au/news/2020-07-15/tech-stock-bubble-warnings-amid-coronavirus-rally/12455410

[51] Ian Brown and Christopher T Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press 2013) 47.

launch e-governance of some kind, they centralise previously separated personal data, creating the potential for much more detailed cross-referencing of databases and, thus, more effective profiling, classifying, and 'guiding' of individuals, their interests, desires and intentions.[52]

The degree of State interference with the right to privacy is growing rapidly in the whole world. Not only China with its infamous legislation on social profiling of citizens, or Russia, are examples of this type of policy. Esteemed democracies such as Sweden are on the same path. We do not seem to have the tools to question or challenge the importance for the State to establish a certain level of control over the population in cyberspace. The security discourse combined with the invisible panopticon and its technological complexity do not lend themselves to bitesize democratic debate. To learn the language, to master the idiom and to study the map of cyberspace cannot be done via services that clip you at 15 seconds (e.g., TikTok) or 280 characters (Twitter). The arguments that are heard are most popularly the security concerns, terrorist threats, other criminal, often 'foreign-based' activities, and human rights violations although the human rights rhetoric is not at the peak of its popularity in most States any longer. However, surveillance does not stop at the point of combating crimes, since the rhetoric of the potential dangers created by cyberspace goes much beyond. As Sky Croeser says, there have been situations in which elites were threatened by activists, such as the inclusion of 'anti-globalization hackers' in US military training scenario[53] and UK attacks on an Anonymous chat channel and specific participants.[54] As Croeser notes, it is much more surveillance than merely an unintended side-effect. Recent responses to Covid-19 crisis have contributed to the increase in surveillance legislation. Individuals are constantly monitored by government agencies: their time out, their movements, the reasons to get outside, their routes, destinations, and their contacts. There are fears of viruses spreading through technological channels and yet more talk on the bad men of cyberspace.

Individuals, however, have a weak understanding of the nature of profiling, contents of personal data, and privacy. At most they have a fear of losing their privacy without giving any definition or limits to it. As Lessig pointed out, the code has already upset a traditional balance when it comes to the notion of private life of individuals and a control that individuals have over the facts of their private data.[55] It is impossible to control what others may know about one when it comes to cyberspace. Lessig uses a digital worm malware as an example. The worm penetrates the computer and searches for particular information, a file or other materials that might be stored there. If it finds the materials, it reports back, if it does not find anything it deletes itself.[56] Most probably, the user of the computer does not notice that the worm has been there unless it is stopped by the antivirus software. The worm's search is easily conducted in a very short time and most likely it does not bother the individual user at all.

It is common knowledge that such searches are being performed on a regular basis by many entities. It is not a secret that people are being actively profiled and that this profiling has an imminent effect on their daily lives. The reactions range from the complete denial of any data

---

[52] Ross Anderson, Ian Brown, Terri Dowty, Philip Inglesant, William Heath and Angela Sasse, *Data-Base State: A Report Commissioned by the Joseph Rowntree Reform Trust Ltd* (2009).

[53] Sky Croeser, *Global Justice and the Politics of Information: The Struggle Over Knowledge* (Routledge 2014) 86–7.

[54] Ibid.

[55] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999).

[56] Ibid.

to any entity, utopian desires to have full control over any profiling activity that is conducted on the internet to indifference often claimed as the 'I have nothing to hide' approach. There is fear and annoyance but there is also a rush to complete the many chores that one can no longer accomplish without the internet. For instance, we clicked on 'accept' quite a number of times without reading the small print when we needed to order groceries online for the family's elderly during the Covid-19 lockdown. Similarly, the corona-tracing apps and bracelets have been adopted as necessary security measures to millions in a variety of countries even at a cost to privacy and there is little knowledge of what will be done with all the data gathered after the threat recedes.[57]

The universal trend to increase surveillance is countered by civil society activists. A cat and mouse chase of sorts has developed. Rapidly evolving technologies allow informed users to be ahead of State agencies in developing businesses and solutions that prey on fears, offer protections against the many threats, and, as a by-product, many myths. Governments that have more limited resources and seek to follow the principles of data protection established by international treaties may come up with harsh regulations, complete bans and restrictions. For instance, the Russian legislator has introduced an extreme countermeasure against anti-surveillance measures, namely, the prohibition of the use of VPNs (Virtual Private Networks) and other anonymisers within the State's territory. The bill was characterised as 'insane' by the Russian Internet Ombudsman, who said that the government's message seems to be that it is 'going to chase the whole country'.[58]

In 2017, the law on VPNs and internet anonymisers (276-FZ) came into force in Russia. The VPN services were banned on sites that the government considers illegal. In addition, the law prohibited search engines from providing links to banned websites and authorised the federal executive authority supervising online and media content (Roskomnadzor) to block certain sites.[59] In 2018, further amendments were made to the Code of Administrative Offenses to establish penalties and Google was given a 500,000 rubles (US$ 6,500) fine. One of the purposes of the fine was to function as a deterrent for other search engines.[60] In 2019, Roskomnadzor demanded that all VPNs, anonymisers and search engines block all websites included on their regularly updated register of banned sites.

Again, it is not only Russia. The UK has long considered proposals to ban strong encryption to private individuals, and, recently, those proposals have been resurrected while the UK government is considering whether to impose a ban on VPNs.[61] Even presently, any VPN service based in the UK is obligated by law to provide information to the police and intelligence agencies when asked to do so since, at the end of 2016, the UK introduced 'the

---

[57] Rishi Lyengar, 'In the Battle against Coronavirus, Privacy is at Risk', *CNN* (20 March 2020) https://edition.cnn.com/2020/03/20/tech/quarantine-privacy-coronavirus/index.html.

[58] 'Internet-ombudsmen nazval "bezumiem" zapret anonimajzerov i VPN', RBK, 2017 (in Russian) https://meduza.io/news/2017/06/08/internet-obmudsmen-nazval-bezumiem-zakonoproekt-o-zaprete-anonimayzerov-i-vpn.

[59] See Human Rights Watch, *Russia: Growing Internet Isolation, Control, Censorship* (18 June 2020) https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship.

[60] Ibid.

[61] Gary (anonymous tech blogger), *What Chance a UK ban on VPNs?* (4 May 2017) https://www.no2id.net/newsblog/2017-05/what-chance-a-uk-ban-on-vpns/.

most extreme surveillance in the history of Western democracy',[62] namely the Investigatory Powers Act.[63] It allows government agencies to access personal data of individuals stored by Internet Service Providers (ISPs) without a warrant. The Act creates heavy surveillance over all activities. As an initial counter-action, according to Liz Kintzele, the informed users in the UK employed VPNs.[64] Lately, the use of VPNs in the UK has increased from around 16 per cent to over 40 per cent.[65] IPA, nicknamed the Snooper's Charter replaced the Data Retention and Investigatory Powers Act of 2014 (DRIPA), which was a temporary Act. The previous Act had been introduced hastily after a European Court of Justice ruling that UK security services could not retain communications data and their actions had been deemed incompatible with EU law by the High Court.[66] Due to the DRIPA having an expiration date, the IPA was conceived hastily and was deemed incompatible with provisions of EU law.[67] There has been a lot of controversy around IPA. In essence, the critics argued that even though the purpose of the Act was to improve transparency, the outcome was the legalisation of bulk government surveillance. An online petition demanding the Act's repeal attracted over 200,000 signatures. However, the petition did not lead to a struggle and it was never debated by the Parliament.[68] The lead advocacy for the IPA was the combating of serious crime. The Act places a duty on communication service providers (CSPs) to keep a record of the websites that their users visit.[69] In 2018, the European Court of Human Rights ruled that the law's lack of supervision on how data was collected was in breach of privacy and human rights law. A ruling by the High Court followed, and it found that the requirement for CSPs by the government to store the record was in direct contradiction to the right to privacy.[70] In the beginning of 2019, some amendments were made. The records can henceforth be accessed by police and other public bodies with either a warrant or for the purposes of tackling 'serious crime' even without a warrant.[71] The problematic Act was brought back to the High Court in 2018 for a judicial review of grounds not previously ruled upon and found that using 'bulk warrants' to obtain and store our information was lawful and appeals are pending.[72]

---

[62] @Snowden, 'The UK has just legalized the most extreme surveillance in the history of western democracy. It goes further than many autocracies', *Twitter* (18 November 2016, 12:59 am). https://twitter.com/snowden/status/799371508808302596?lang=en.

[63] https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

[64] As cited by Peter R Allison, 'Challenges of the Investigatory Powers Act', *ComputerWeekly.com* (25 January 2017) http://www.computerweekly.com/feature/Challenges-of-complying-with-the-Investigatory-Powers-Act.

[65] Rhys Gregory, 'More UK Citizens are into VPNs, and They are Justified', *Wales 247* (8 October 2020) https://www.wales247.co.uk/more-uk-citizens-are-into-vpns-and-they-are-justified/.

[66] Dale Walker, 'What is the Investigatory Powers Act 2016?', *IT Pro* (6 July 2020) https://www.itpro.co.uk/policy-legislation/33407/what-is-the-investigatory-powers-act-2016.

[67] Ibid.

[68] Ibid.

[69] See ibid and Scott Carey, 'The Snoopers' Charter: Everything you need to know about the Investigatory Powers Act', *Computer World* (31 July 2019) https://www.computerworld.com/article/3427019/the-snoopers-charter-everything-you-need-to-know-about-the-investigatory-powers-act.html.

[70] 'Deadline to Amend UK Surveillance Laws', *BBC News* (27 April 2018) https://www.bbc.com/news/technology-43928147.

[71] A crime that would receive a minimum sentence of one year.

[72] Liberty, *Court Judgement Allows the Government to Continue Spying On Us* (29 July 2019) https://www.libertyhumanrights.org.uk/issue/court-judgement-allows-the-government-to-continue-spying-on-us/.

The use of technological countermeasures does not help with the politics of fear, which mark both the cat and the mouse in the chase, and thus every action and counteraction. The escalation into another episode in the war of technologies further feeds the fears and produces more myths about dangers, risks and terrorism. The war in turn buttresses the myths to the point of making them self-fulfilling prophecies. The Crypto Wars, again very similarly to the Thirty Years War analogy, have many disconnected fronts and battles that cannot be reduced merely to the privacy-surveillance debate.

As a consequence, there are so many fears and threats that many resign into indifference. While some assume the 'I have nothing to hide' approach, others choose the question: 'Do I have anything to share?' Self-disclosure is an aspect of autonomy and can be done on many different levels: one can disclose one's name but not their salary or political affections. The so-called data mining and cross-referencing technologies, however, often frustrate such levels and distinctions: names, ages, places of birth or study, shopping habits, diets, pictures, holiday destinations, other people contacted, and Google searches can be harvested and combined. In the extreme, the disclosure penetrates into the most intimate spheres of one's life either driving even deeper fears or encouraging sexualised fantasies of being totally exposed, open and shared by the whole world – nude without the veil and penetrable without even the 'skin' provided by encryption. Therefore, as Mireille Hildebrandt points out, the crucial distinction between volunteered and observed/harvested data does not seem sufficiently clear.[73] In Hildebrandt's words, volunteered data is something that is deliberately provided, e.g., name, age or a place of work submitted to social media. The *problematique* of digital consent and its relationship to any free will remains to be rehearsed in cyberspace. In a different context, in cases of date rape, pro-victim advocates have fought a long battle to get a robust or genuine consent recognised and, indeed, to turn the focus to imbalances of power rather than insist on a formal but empty 'consent';[74] as to cyberspace such a debate has not even properly started yet.[75]

Observed data is information that is not consciously provided by an individual. It is behavioural data collected by, for instance, an application (app) on the mobile phone. A person might agree to a service capturing such data, but that does not imply that they are deliberately providing this information. The devil is in the detail, and here it is in translation. Volunteered data is what people think they do, observed data is what they really do.[76] Volunteered data is what people do not want to hide, observed data is what they perhaps are not ready to share, or in the worst-case scenario, something that they do not even know about themselves. Hence, profiling implies some entity (governmental or commercial) collecting very detailed information on behaviour that can be, with relative effort, translated into knowledge of the subjects' deep fears, desires and thoughts. As Hildebrandt notices, that goes even further with pre-emption measures,[77] which goes one step ahead of profiling. It anticipates our actions based on a large number of collected observed data, simultaneously eliminating our own anticipations as

---

[73] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Edward Elgar 2016) 32.

[74] See e.g., Michal Buchhandler-Raphael, 'The Failure Of Consent: Re-Conceptualizing Rape As Sexual Abuse Of Power' (2011) 18 *Michigan J. Gender and L.* 147, 198.

[75] See Marie-Helen Maras and Adam Wandt, 'Enabling Mass Surveillance: Data Aggregation in the Age of Big Data and the Internet of Things' (2019) 4 *Journal of Cyber Policy* 160; Dag Wiese Schartum, 'Making Privacy by Design Operative' (2016) 24 *International Journal of Law and Information Technology* 151.

[76] Hildebrandt (n 73) 32.

[77] Ibid., 51.

unnecessary and inaccurate.[78] This is the point when quantitative data becomes qualitative, though not necessarily reflective on IRL-situation. As the numbers are not used in a context, there are unavoidable flaws leading to assumptions, increased discrimination, social division and negative consequences for non-privileged groups, which again circles back to the threats and fears camouflaging the underlying power dynamics of the algorithm-driven cyber realm.

There is yet another consequence, namely the loss of trust in cyberspace and an attempt to deny technological involvement in one's daily life. Sceptics ask whether we will ever become internet beings meaning that our social and cultural forms – including our norms – may not be transportable to cyberspace. For others it seems that the new generations born in the era of the Internet of Things (IoT) or Internet 3.0 can only be truly 'netizens' of the cyber realm (citizens of the 'net') – and there is no harking back to the analogue age. Such a generational divide implies the division of humanity: the genuine netizens and those who either refuse or try but will never have the same relation to the internet as the netizen-generations. Such a digital gulf-view of divided humanity is often marked by leaving the oldies and the poor behind and embracing the new era as inevitable, general, casual, firmly present in the everyday discourse beyond further onto-epistemological questioning. One may claim that it is impossible to avoid the connection to the cyber realm: we communicate, work, shop, and gain information through digital technological means. In the latter view, one may yet make divisions within the cyberspace; for instance, one may avoid particular providers, platforms or services that are labelled as criminal, conspiratory or controlled by some evil other, e.g., the myth, popularly held in Russia, that the internet is a CIA creation and thus dangerous in every domain except one's own. The fears lead to myths; these lead to the cat and mouse chase and stereotypes which we see performed in US-China, Russia-EU, West and the Rest relations. The power of expert rhetoric prevents transparency and we respond in various ways: resistance, annoyance, frustration, division, resignation or devil-may-care.

5. POWER EMBEDDED IN TECHNOLOGY ETHICS DISCOURSE

'Technology is neither good nor bad; nor is it neutral' is still a valid imperative.[79] There is no question that money is poured into military technology development and that technology transfer is problematic for the Global North. Yet, technological investments are an axiomatic, unquestionable part of the economy of eternal growth. Even the sustainability discourse has incorporated concepts such as green tech, clean tech, dem tech and green growth – to steer away from radical economic governance or slower digitalisation.[80]

As to the fundamental questions, the cyberspace discourse lacks precision and fosters strategic ambiguity.[81] For instance, the regulation of artificial intelligence (AI) is often debated

---

[78] Ibid.

[79] Melvin Kranzberg, 'Technology and History: Kranzberg's Laws' (1986) 27 *Tech. & Culture* 544, 545.

[80] For more specific information on sustainability transitions, green growth and economics, see e.g., Marco Capasso, Teis Hansen, Jonas Heiberg, Antje Klitkou and Markus Steen, 'Green Growth – a Synthesis of Scientific Findings' (2019) 146 *Technol. Forecast. Soc. Change* 390.

[81] See Agre (n 10).

on the basis of the technology's ethical implications. However, the AI ethics discourse is wickedly confused;[82] e.g., the question of whether AI is *ethical* means very different things in various contexts. For some, it entails the ethics embedded in the technology itself, whereas for the majority of ethics scholars, it connotes the ethics and morals that humans apply vis-à-vis digital technologies, their research, development and use in the political economy.[83] The former (minority) position, however, challenges the latter in different ways e.g., through non-human cognition, hacker ethics-based views and the code-as-law thesis. However, seen from a 'quotidien phenomenology' perspective, digital technology creations whether AI, other bots or 'things' residing in the emerging IoT lack ethical capabilities because they lack the human bodily experience, consciousness of moral status and dignity, self-determination, autonomy and open existentiality which they cannot but simulate unless they make a huge qualitative leap.[84] The so-called *post-singularity* activists see such a leap looming in the near future. Also known as *AItheism*, this position predicts that artificial super-intelligence (ASI) overtakes and overpowers human capabilities in all respects by 2030/2045,[85] which would also revolutionise ethics through disrupting the status of the human person as the main ethical agent and the setter of the frame of reference for ethics and morals. The minimalist, on the other extreme, sees that AI even at its most developed will take over ever more of the formalised and formalisable activity leaving the non-formal for the humans.

Most often, rapid technological development and ethical considerations do not develop side-by-side. Such seems to be the case also with the IoT and ethics. Instead, automatic task performing internet bots, things 'imitating intelligent human behaviour (AI)'[86] or other devices connected to the IoT call for reflection of ethical issues. Especially IoT's underdeveloped security raises ethical worries of e.g., privacy, informed or robust consent, informational security, safety and trust.[87] Yet, the ethical debates are often conducted among governance experts and rehearse such familiar and formal solutions as the creation of a new guideline for new technologies, the essence of which is that they have to respect human dignity and comply with existing human rights – which are first to be reduced to quantitative language and therethrough to code. The new human conditions brought about by the intertwining of the cyber with the IRL, as in the case of AI, pose challenges that are ontologically different and thus incommensurate with such coded bills.[88]

---

[82] Ibid.

[83] Jaana Parviainen and Juho Rantala, 'The Implementation of AI Platforms to Automate Decision-Making in Expert Organisations: Reconsidering the Principles of Professional Ethics in the Age of Algorithms' (2020) Paper Presentation at 36th EGOS Colloquium: Organizing for a Sustainable Future: Responsibility, Renewal and Resistance, 2–4 July 2020, Hamburg, Germany.

[84] John Brockman (ed), *What to Think About Machines That Think: Today's Leading Thinkers on the Age of Machine Intelligence* (Harper Perennial 2015); Maija-Riitta Ollila, *Tekoälyn etiikkaa* (Otava 2019).

[85] Raymond Kurzweil, *The Singularity Is Near: When Humans Transcend Biology* (Viking 2005).

[86] For a definition of AI see Joost N. Kok, Egbert J W Boers, Walter A Kosters and Peter van der Putten, 'Artificial Intelligence: Definition, Trends, Techniques and Cases' in *Artificial Intelligence*, Vol. 1 *Encyclopedia of Life Support Systems* (EOLSS) 1–21.

[87] Fritz Allhoff and Adam Henschke, 'The Internet of Things: Foundational Ethical Issues' (2018) 1–2 *Internet of Things* 55.

[88] See Matilda Arvidsson, 'The Swarm that we Already are: Artificially Intelligent (AI) Swarming "Insect Drones", Targeting and International Humanitarian Law in a Posthuman Ecology' (2020) 11 *Journal of Human Rights and the Environment* 114.

The non-human cognition theory recognises that even fauna, flora as well as IT possess cognitive faculties on the condition that 'thinking' need not necessarily be anthropocentrically defined. Consequently, non-human cognition is also recognised as a meaning-giving instance, which makes non-human ethics conceivable.[89] Hacker Ethics, on the other hand, foregrounds collective creativity, collaborative problem-solving, and decentralised, internet-based search for solutions for all kinds of problems, also ethical. It pulls together human coders and thinkers through digital internet communications in a symbiotic way that is radically different from the activity of the traditional moral agent i.e., the autonomy-capable individual bodily subject. The significance of this difference fuels the debates about the moral permissibility of algorithmic war and targeting e.g., by drones and other autonomous weapons systems. Thirdly, the code-as-law idea embeds normativity within the technical code and the mathematical algorithm; which, logically, also entails at least some kind of non-individual and technologically assisted prescription that is one definition of a simple form of ethics. According to this view, norms must be designed to guide the culture of coders. According to it, our best vision is the culture of formalism/culture of code(rs), as suggested above.[90]

The non-neutrality of digital technologies is often obscured if one is carried away by the various dys- or utopia. The key concerns of our society relate to the *datafication* of life, which entails interrelationships and impact flows among technology, economy and politics. By surveillance capitalism, some critics refer to the exploitation of human data traces for the purposes of hyper-consumerism.[91] Others criticise the emergence of the unprecedented, highly unpredictable and non-transparent power concentrated in global giant data enterprises, the GAFA, the main representatives of platform capitalism.[92] These developments both promote the social, economic and consumerist interests of the wealthy, and divide more and less important persons into segments that are constituted by risk analysis and probability algorithms designed to separate the valuable from the valueless, the healthy from the sickly by grading systems and indicator-based calculi. The combination of personal data traces from various sources are 'mined' by specialised actors without the knowledge of the concerned individuals and often also unbeknown to the companies from whose databases the information is drawn. Only rarely ethical concerns are raised in this connection. The data mining constructs digital footprints or, more robustly, *digital doubles* of human individuals that are used in all kinds of eligibility decisions e.g., for educational institutions, insurance, credit, employment, housing, health care, pension, benefits, access, visas, eligibility to travel *ad infinitum*.[93] Such classification inevitably veils and exacerbates societal inequalities and polarisations. And, as to consent, there are not many who would wish to forgo the entry to such institutions and services through exercising their right to refuse consent to various data collectors. The ethical stances to the various questions arising in cyberspace should be investigated in their rich contexts, carefully considering the radical differences but also the similarities vis-à-vis the physical world. A situated ethics of encounter, the intertwined technological, political and economic stakes, and

---

[89] N Katherine Hayles, *Unthought: The Power of the Cognitive Nonconscious* (University of Chicago Press 2017).

[90] Agre (n 10).

[91] Shoshana Zuboff, *The Age of Surveillance Capitalism. The Fight for the Future at the New Frontier of Power* (Profile Books 2019).

[92] Outi Korhonen and Jari Ala-Ruona, *Regulating the Blockchain* (Liikejuridiikka 2018) 77.

[93] Virginia Eubanks, *Automating Inequality How High-Tech Tools Profile, Police, and Punish the Poor* (St. Martin's Publishing Group 2018).

the changes of subjectivities, agency and concepts of cognition help to tackle if not solve the otherness of the cyber questions.

6. CYBERSPACE AS COMMONS AND SITE FOR EMPOWERMENT

Cyberspace remains an angst-creating or an exciting jungle of mythical minotaurs and stealthy creatures. Cyber realism as the midway position holds that there is no cause for excitement since all is the same as ever in the world of management and governance whether we focus on concrete objects or digital bits. Governance technocratic measures can list support through the allure of participation with the tech-elite or through the mass politics of fear, control, war, division and discrimination. The tech-elite, the informed users and internet experts, speak of the internet as a new architecture to be governed by post-Westphalian models.[94] David Kennedy, who has written widely on international law and governance as disciplines of renewalism, identifies the moments of progress with the proliferation of new institutions, maps, plans, geometries, architectures and political alignments, which, for instance, in the wake of the 1989 shift were publicised and debated widely in the media.[95] Often, the renewal is more a case of the Emperor's new clothes. On the other hand, radical shifts may also take place in hushed and obscured terms, as in the case of the gradual federalisation of the European Union in the field of civil law, as discussed by Helen Hartnell;[96] or the build-up to the 2008 crisis in global finance, as Kennedy put it: 'Indeed, as the … financial crisis demonstrates, global governance remains a mystery … [S]imply mapping the channels and levers of influence … remains an enormous sociological task.'[97] This chapter claims that it is high time to raise not only sociological but general awareness and discussion on the maps, designs, architectures and architects, in particular, as regards cyberspace. The power asymmetries of the real world have been partly exacerbated and partly skewed out of recognition in the cyber landscape of business actors, transnational multi-State actors, transnational private actors and civil society groups and movements taking new roles besides governments and traditional intergovernmental organisations.[98]

Cyberspace is inherently global and what is meant by 'local' is different therein than in the IRL. It is global to the extent that it would seem logical to devise some kind of a commons arrangement, an Outer Space or Antarctic-like treaty or an International Seabed Authority (ISA) kind of an agency, to harvest and redistribute certain gains and to affirm our commitment to freedom, peace, security and cooperation beyond sovereignty. In the style of the modern framework processes, yet without a treaty, the inter-governmental and multistakeholder effort at Internet governance (IGF, Internet Governance Forum) proclaims the freedom, respect for human rights and sustainable development goals together with a number of controversial

---

[94] Leiser and Murray (n 19) 2–3, 32.

[95] David W Kennedy, 'Turning to Market Democracy: A Tale of Two Architectures' (1991) 32 *Harv. Int'l L. J*. 373, 377.

[96] Helen Hartnell, 'EUStitia: Institutionalizing Justice in the European Union' (2002) 23 *NW J. Int'l. Law & Bus*. 65.

[97] David W Kennedy, 'The Mystery of Global Governance' (2008) 34 *Ohio N.U. L. Rev*. 827.

[98] Ibid.

visions.[99] Yet, there is no global commons talk[100] and no Tobin tax[101] kinds of initiatives in the intergovernmental organisations.

The digital organisations rallying for public benefit tend to be grassroots or private initiatives, such as many emerging decentralised autonomous organisations (DAOs). These are new organisational modes whose constitutional makeup both in technological and governance terms varies greatly and has not stabilised. DAOs (not to be confused with 'The DAO' – a particular experiment) differ from traditional legal subjects but can be seen as a derivation of cooperatives. Matthieu Quiniou has defined DAO as 'an autonomous and decentralized organizational system whose rules of operation and participation are provided for by a smart-contract registered in a blockchain'.[102] DAO's method of operating does not rely on human intervention but instead on a self-executing code placed on a blockchain, and it can operate towards its coded ends, arguably, with or without human governance.[103] The nature of a DAO therefore enables new possibilities for participation and organisation.[104] There are a number of DAOs raising funds for and committed to ecological preservation with minimum human opportunism. Some DAOs propose a market for sovereignty, identity cards, marriage licenses and dispute resolution.[105] Others seek to empower grassroots movements with finance and their own coin systems. DAOs are potentially new subjects that might transform the landscape of cyberspace and thus alter its power relations through digitally enabling more efficient and more widely distributed operations for varieties of social movements. Yet very few among the public have ever heard of them.

The Internet Governance Forum Annual meeting in Berlin in 2019 was titled 'One World. One Net. One Vision' yet the keynotes (Guterrez, Merkel) called for 'a free, open, and decentralized Internet'.[106] Freedom and decentralisation stands in contrast to the ideal of just one vision, which quite obviously is not present. The Forum labours under the same problems and controversies that prevented the International Telecommunications Union (ITU) from receiving the support of the EU and the West for an updated International Telecommunications Regulation (ITR) some years ago; with 89 non-Western signatories the 2012 ITR was rejected by 55 States following the lead of the US and Google, who deemed it as an attempt to increase government 'censorship' of the cyberspace[107] despite the fact that the ITR does not even mention the internet. The suspicion and mutual blaming told of a very divided agenda. In the IGF's 2019 proclamation of unity and oneness we can hear an oxymoron: a totalitarian liberalism of one vision of freedom.

While the heads of State, numerous NGOs, industry representatives and foundations engage each other on the global forum producing UN-style language of respect and good-

---

[99] On human rights and cyberspace see Fidler (Ch 7 of this Handbook).

[100] See Tsagourias (Ch 1 of this Handbook).

[101] See e.g., https://www.europarl.europa.eu/workingpapers/econ/107_en.htm?redirected=1.

[102] Matthieu Quiniou, *Blockchain: The Advent of Disintermediation* (ISTE 2019) 85.

[103] Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018) 148–50.

[104] See e.g., Hsieh, Ying-Ying, *The Rise of Decentralized Autonomous Organizations: Coordination and Growth within Cryptocurrencies* (2018) Electronic Thesis and Dissertation Repository, https://ir.lib.uwo.ca/etd/5393.

[105] See https://tse.bitnation.co/.

[106] See https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/9212/2172.

[107] See https://phys.org/news/2012-12-nations-controversial-telecom-treaty.html.

will, the governance and the design decisions of cyberspace take place elsewhere. With the intergovernmental and multistakeholder measures lacking progress, governance is deferred to the engineering and technical standards organisations. The ISOC (Internet Society) provides leadership in internet standards, consultation and policy. The IETF (Internet Engineering Task Force) consults on the technological design, use and management. The IAB (Internet Architecture Board) consults and exercises oversight on internet architecture together with both of the former agencies. As argued at the beginning of the chapter, these interact, finance and agree on standards and solutions that shape the cyber realm. They enable the dominance of those sectors as an unquestioned given – military, global finance, electronic commerce – whose acquisitions of cyberspace we cannot see and to which we thus pay little if any attention. They rule by expertise, standards and allocation of domain; their standards may not be legal but they become economically mandatory because no minority group or actor can afford fighting an established standard. Those who try will fare similarly to Russia, China or North Korea, who occasionally attempt it.

A number of the informed citizens surely pay attention to the widely publicised efforts of the IGF to command respect for the sustainable development goals, and the ensuing frustrations and controversies. However, these are the same goals and ideals that pertain to the governance of climate change, free trade and the oceans, and, thus, so general, that they do not help to ease our anxiety with the everyday issues including privacy, opportunity and belonging. Meanwhile, in the background, the technical community makes vastly important decisions gauged in the expert Latin of algorithms and bits that affect the distribution of wealth and resources related to or to be gained by means of cyberspace – outside our focus. Kennedy has written widely on the background power of experts and their rule arguing that:

> everyday decisions made by the professionals who manage norms and institutions which seem to lie in the background of global politics may be more important to wealth and poverty than what we customarily think of as the big political and economic decisions made by parliament and presidents or brought about by war and peace…[108]

This seems particularly true for cyberspace, which has rapidly developed without the large majorities of the global public having any idea about the social, political or economic directions of this development.

The most influential cyberspace agency may be the ICANN (Internet Corporation for Assigned Names and Numbers) that governs the 'root' i.e., the addressing and domain name system (DNS) and thus also the taxonomy of cyberspace. The ICANN was created by the Clinton Administration in 1998 as a privatisation operation of the internet addresses system. The US government transferred the so-called 'IANA function' of internet address blocks that had previously been managed from an institute within the University of Southern California to ICANN.[109] It is a highly powerful private regulator with a global reach that takes advice from governments yet the ICANN Board decides independently; it can select which internet identities it issues and deletes, and the conditions under which they can be operated. The IRL-analogy would be a single global agency that decided whether you can have a home

[108] David W Kennedy, 'Challenging Expert Rule: The Politics of Global Governance' (2005) 27 *Sydney L. Rev*. 5.

[109] See Leiser and Murray (n 19) 15, 32.

address, nationality, and whether you are permitted to interact with others. We would not accept such a concentration of power in IRL. The ICANN has been criticised, on the one hand, for its lack of accountability, transparency and privatised nature, and on the other, on having maintained a close link with the US administration. As the only government, the Obama Administration sought to gain a veto-power in it but failed.[110] Despite its power and high profile, it remains invisible, incomprehensible and in the dead zone of the main news media. The creation and the appointment of the office of the Independent Objector (currently held by international law expert Alain Pellet) has done little to make it known to the global internet users, whose 'best interests' he serves with the right to object to but not to veto the Board.[111]

It is these agencies, architectures and designs that provide the governance map of cyberspace. In Lessig's words:

> What the architecture enables, and how it limits its control, are choices. And depending upon these choices, much more than regulability will be at stake (…) Thus whether (for instance) the certification architecture that emerges protects privacy depends upon the choices of those who code. Their choices depend upon the incentives they face.[112]

Very few of the users or even the legal experts can identify what the choices are, let alone the incentives, and what the role of privacy in the field of encryption, and further, the fate of encryption in the larger questions of borders of control, identity and the Cyber War are. One Independent Objector cannot remedy it.

7. CONCLUSION

The problem in cyberspace governance today is that the architectures, architects and the choices in the background remain effaced. Their rich context embraces the cyber but also the IRL realms. They are distinct but also overlapping and interdependent, remaining unsituated and thus disconnected from our life-world and from the political economy surrounding us. This chapter urges that we abandon fear, denial, resignation and cyber realism based cyberspace governance discourses to forge a discussion and start mapping the architectures and designs, and identifying the architects, deciphering their grammar and learning the topics of debates beyond 'security v. privacy'. Our protestations of activism against the securitisation of the cyber realm will have no chance to succeed if we do not have a map of the terrain, know the language, interest ourselves in the culture created by the cyberspace giants and background actors; learning about their background stories, their language and tools that they tend to use in the private and the public side of their activities is mostly lacking. In order to grasp transformative potential, we would have to situate the debates in rich global political contexts and relate them in concrete terms to the emerging cyber-intertwined human condition of our everyday lives.

---

[110] Ibid.

[111] Ibid. 17, 32.

[112] Lawrence Lessig, 'Code is Law: On Liberty in Cyberspace', *Harvard Magazine* (January–February 2000) http://harvardmagazine.com/2000/01/code-is-law-html.

4. Jurisdiction in network society

Uta Kohl

1. INTRODUCTION

After two and a half decades of confronting emergent global network society, it may fairly be said that governments have, once again, found their regulatory mojo. Although the ease of transnational activity by any Joe Bloggs continues to challenge territorially conceived law and order, network society also offers significant new opportunities for the State to reassert its authority, and even deepen it, and thereby reconstitute territorial sovereignty. Yet, these new opportunities have also created new jurisdictional boundary areas that can and have been contested on the basis of illegitimate extraterritoriality.[1]

These new opportunities lie, *in the first place,* in the presence of a dozen dominant global platforms (most prominently the Big Five[2]) whose dependence and interest in stable, legally secured trading environments make them, ultimately, natural allies and cooperative partners of State authority – regardless of their occasional legal squabbles and the undoubtedly real conflicts of interests.[3] The jurisdictional cases discussed below in which global platforms seek to resist regulatory expectations and gatekeeper responsibilities under State law, should be understood as part of the negotiation between State and platform through which their relationship is settled, rather than as contestation of State authority per se. These negotiations involve, as a matter of real-politic, two relatively equal parties, even if the State as public authority has, on a constitutional register, the upper hand over any private actor no matter its size. Facebook's threat to withdraw from the EU,[4] following the CJEU's decision to strike down, once again, the Privacy Shield (2020)[5] that sought to legitimise the transfer of data to the US, pointedly communicates the bargaining strength of the social media platform that has become a staple communication medium for millions. Facebook's withdrawal from the EU would almost certainly cause significant economic and political disruptions, protests and legal challenges, and would ultimately require compromise by public authority. By the same token, the centralisation of network activity through these platforms (contrary to early narratives of decentralisation and disintermediation) gives them an ideal vantage point for 'ordering' online activity, which they inevitably do through their design choices and Terms and Conditions, and which States have only too readily seized upon. On a different note, the European Court's

[1] Julia Hörnle, *Internet Jurisdiction Law and Practice* (OUP 2021) Chapter 6.

[2] Google, Microsoft, Apple, Amazon and Facebook, although there are others e.g., Twitter, eBay.

[3] David Morley, Kevin Robins, *Spaces of Identity – Global Media, Electronic Landscapes and Cultural Boundaries* (Routledge 1995) 223 (noting interests of transnational corporations in the free flow of information across the world market).

[4] Alex Hern, 'Facebook says it may quit Europe over ban in sharing data with US', *The Guardian* (22 September 2020) https://www.theguardian.com/technology/2020/sep/22/facebook-says-it-may-quit-europe-over-ban-on-sharing-data-with-us.

[5] *Data Protection Commission v Facebook Ireland and Maximillian Schrems*, Case C-311/18 (CJEU, 16 July 2020).

decision on the invalidity of the Privacy Shield also reaffirms States' unwillingness to freely share the data of its residents with 'foreign' public authority, here the US. It implicitly underscores that cooperation between States is acceptable within strictly agreed limits and ideally on a reciprocal basis, as opposed to any wholesale informal data flows facilitated by private actors. In short, judicial pronouncements and legislative initiatives addressing online transnationality may generally be read as settling aspects of the tripartite relationships between State and global platform *and* between States inter se. Notably, it is only the latter relationship that customary international law in general, and on jurisdiction specifically, sees and acknowledges. Private actors – no matter their size, de facto alliance with public authority or regulatory importance – are prima facie outside the classic purview of public international law. Their invisibility in public international law at once heightens their freedom of action in the global sphere, and arguably also their potential usefulness to States as vehicles for regulatory intervention outside the legal accountability that attaches to public authority at the domestic and international level.

Second, new opportunities for regulatory oversight, law enforcement and social control also arise from the availability of the large personal data sets that are generated by network participants in the course of using the network and its myriad applications. Although the data is, in the first place, collected and commercially exploited by private actors (again with the dominant platforms playing a key role), it then also becomes available to public authorities. The GDPR (2016)[6] that has been celebrated as a major success for informational privacy, excludes from its scope any processing of personal data 'by competent authorities for … the prevention, investigation, detection or prosecution of criminal offences … including the safeguarding against and the prevention of threats to public security'.[7] At the same time, it also creates wholesale rights exemptions for the sharing of personal data held by private actors with 'competent authorities' for the purposes of crime prevention, detection and investigation.[8] These secondary 'public' uses of the personal data sets range from *reactive* uses of e.g., personal phone data in criminal prosecutions, to *proactive* monitoring of network behaviour through mining to predict criminal or disorderly activity from terrorism to, potentially, much more low-level anti-social conduct or political protests. For example, Google was served with a search warrant to release data sets in a murder investigation in Arizona in 2018,[9] whilst Apple health data app provided evidence in a murder prosecution in Germany in the same year.[10] Meanwhile 23andme and ancestry.com, public genealogy sites with databases of mil-

[6] General Data Protection Regulation 2016/679, in force since 25 May 2018.

[7] Ibid., Recital 19. Criminal, as opposed to administrative offences, are governed by Law Enforcement Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. For a critical commentary on the blurry boundaries between the GDPR and the Law Enforcement Directive, see Mireille M Caruana, 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement' (2019) 33 *International Review of Law, Computers & Technology* 249, 253 *f.*

[8] See Data Protection Act 2018, Part 3 and Sch 2 and 3, see also s 30 and Sch 7 on 'competent authorities'. ICO, *Data Sharing Code of Practice – Draft Code for Consultation* (15 July 2019) 62 *ff.*

[9] Alex Welsh, 'Tracking Phones, Google is a Dragnet for the Police', *New York Times* (13 April 2019) https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html.

[10] Stephen Jordan, 'Apple Health App Data Being used as Evidence in Murder Trial in Germany', *Digitaltrends* (14 January 2018) https://www.digitaltrends.com/mobile/apple-health-app-murder-germany/.

lions of DNA profiles, have been forced to open their sites to police searches.[11] These are isolated examples of widespread, substantial and sustained access requests by public authority in relation to the personal data held by platforms – as made visible in their transparency reports.[12] This comes in addition to the bulk monitoring of personal data by public authority,[13] with the willing or reluctant cooperation of private providers, as most notoriously revealed by Edward Snowden's whistleblowing on mass surveillance by US and UK intelligence agencies.[14] There are also instances of open voluntary cooperation. For example, Amazon has publicly partnered with more than 400 police departments in the US to give them access to doorbell camera footage on its platform in return for the police promoting its 'smart' doorbells.[15] In all the above scenarios, access to large privately collected sets of finely pixelated digital footprints offers unprecedented opportunities for deepening territorial law and order. Problematically from a jurisdictional perspective (in addition to any privacy concerns), these data sets are profoundly infused with transnationality. On the one hand, they tend to be controlled by global US-based platforms and, on the other, data as an intangible, slippery commodity does not seem to be easily territorialised for the purposes of jurisdiction. Still, much like in earlier internet jurisdiction cases with their main focus on harmful content,[16] regulatory entitlement can be, and has been, asserted on the basis of the data's relational link with the territory. Indeed, it

---

[11] Jocelyn Kaiser, 'A Judge said Police can Search the DNA of 1 million Americans Without their Consent. What Next?', *Sciencemag* (7 November 2019) https://www.sciencemag.org/news/2019/11/judge-said-police-can-search-dna-millions-americans-without-their-consent-what-s-next; Christopher Slobogin and James Hazel, 'A World of Difference?': Law Enforcement, Genetic Data and the Fourth Amendment (2020) 70 *Duke Law Journal* 705.

[12] See, e.g., Google's transparency report: https://transparencyreport.google.com/user-data/overview?hl=en_GB . Note these reports generally exclude requests by intelligence agencies.

[13] UK Government, *Operational Case for Bulk Powers* (2016); David Anderson, *Report of the Bulk Powers Review* (August 2016) para 8.36: 'In some areas, particularly pattern analysis and anomaly detection, no practicable alternative to the use of BPDs [bulk personal data sets] exists. These areas of work are vital, since they can provide information about a threat in the absence of any other intelligence seed.' Daragh Murray, Pete Fussey, 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data' (2019) 52 *Israel Law Review* 31. On the illegality of the bulk interception of communications by GCHQ, see e.g., *Big Brother Watch and Others v the United Kingdom* A, pp No 58170/13, 62322/14 and 24960/15 (2018) ECHR 299 (13 September 2018). On cyber espionage and international law see Buchan and Navarrete (Chapter 11 of this Handbook).

[14] Claire Cain Miller, 'Tech Companies Concede to Surveillance Program', *New York Times* (7 June 2013) https://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html; see also Paul De Hert, Johannes Thumfart, 'The Microsoft Ireland Case, The Cloud Act and the Cyberspace Sovereignty Trilemma. Post-Territorial Technologies and Companies Question Regulatory State Monopolies' in Walter Hötzendorfer, Christof Tschohl, Franz Kummer (eds), *International Trends in Legal Informatics. Festschrift for Erich Schweighofer* (Weblaw AG 2020) 373 (on the attempt by companies, here Microsoft, to reposition themselves after the Snowden revelations).

[15] Kari Paul, 'Amazon's Doorbell Camera Ring is Working with Police – and Controlling What They Say', *The Guardian* (30 August 2019) https://www.theguardian.com/technology/2019/aug/29/ring-amazon-police-partnership-social-media-neighbor.

[16] Arguably 'data' provides the building blocks for 'information' which in turn provides the foundation for knowledge. James Curran, *Media and Power* (Routledge 2002) 64 *f*, commenting that in medieval Europe the papacy's control over the church, the then main agency of mass communications, meant that it dominated institutions of ideological production and could thereby promote a construction of reality that legitimised its supremacy.

might be posited that territoriality, as a legal and political *construction*, is peculiarly suited to capture intangible assets like data or information.

The above two fields of regulatory opportunities opened up by network society provide the new contextualisation against which judgments and legislative activities dealing with online transnationality may be read. On a substantive level, they manifest a State's 'internal' interest in effective governance, for and of its population, including the protection of security, liberties and economic interests, and its 'external' interest in positioning itself as well as possible in a competitive community of States. In global network society, the realisation of both objectives hinges – as a matter of process and instrumentalities – on the cooperation of global digital platforms as regulatory gatekeepers and as collector of vast sets of personal data. This chapter examines if, and how, customary international law on jurisdiction navigates the realisation of these interests and how in turn these developments shape, or are likely to shape, customary international law.

2. CUSTOMARY INTERNATIONAL LAW ON JURISDICTION

The rules of customary international law on jurisdiction are, with some exceptions, strongly territorially oriented, or location focused.[17] Despite that overarching commonality, their relative restrictiveness varies depending on the type of regulatory competence a State purports to exercise: adjudicative or legislative competence or, alternatively, enforcement jurisdiction, with the distinction broadly aligned to the three arms of government.[18] The *former* concerns the issue whether a State may extend its law and court processes to transnational activity. In criminal cases, unlike civil cases, adjudicative and legislative jurisdiction coincide in so far as a court that decides to go ahead with a criminal prosecution always applies local, and never foreign, law to the case. So generally no distinction is made between adjudicative and legislative jurisdiction under customary international law [hereafter for simplicity 'legislative jurisdiction'] – even if some have argued that a sole focus on limiting adjudicative jurisdiction pays insufficient regard to the effect of too expansive legislation on, e.g., transnational corporate actors which may take defensive steps to pre-empt adjudication.[19] The *latter* type of jurisdiction concerns the question of how far a State's law enforcement processes may reach over and beyond its territory, and is, unlike the prescriptive and legislative jurisdiction, subject to clear territorial limits.

In the online context, the question of whether and when a State's law and court processes can be extended to transnational activities has been raised in innumerable contexts.[20] Can US internet gambling prohibitions reach Antiguan online gambling providers; should a Chinese

---

[17] Apart from the territoriality principle which, as shown below, is also heavily used in the transnational context, the principal bases of jurisdiction are the nationality principle, the protective principle, the universality principle and the passive personality principle. See Cedric Ryngaert, *Jurisdiction in International Law* (OUP 2015) Chapter 4.

[18] See Michael Akehurst, 'Jurisdiction in International Law' (1972–73) 46 *British Yearbook of International Law* 145. See also Luc Reydam, *Universal Jurisdiction – International and Municipal Legal Perspectives* (OUP 2003) 25 *f*.

[19] Ivan Shearer, 'Jurisdiction' in Sam Blay, Ryszard Piotrowicz and Martin Tsamenyi (eds), *Public International Law – An Australian Perspective* (OUP 2005) 154, 156.

[20] The examples are all based on real cases, discussed below.

news site with the domain name of cnnews.com (i.e., cn being the Chinese country domain) have to respect US trademark law; can EU data protection standards be applied Google Search; should US-based Yahoo! Inc have to comply with French or German laws on Nazi memorabilia; can a Dutch pharmacy offer drugs online to German customers if not licenced in Germany; or should a foreign music and film piracy site have to observe the laws of the States where its users are? These issues raise questions as to what a State can legitimately expect and, conversely, what obligations online actors have and should have under foreign law. In any of these cases, if the answer to the question as to whether a State can regulate a foreign-based activity and actors is affirmative, the next question is if, and how, this regulatory assertion can be enforced or implemented. On a related note, the ambit of enforcement jurisdiction may also be invoked at an earlier stage of the criminal investigation, where the criminal activity may have been entirely local but the data evidence lies abroad.

Permissive on Prescriptive and Adjudicative Jurisdiction

A State's decision on the reach of its laws and court processes over transnational activity is *prima facie* a decision made and actioned *within* its territorial boundaries that has no direct impact on the territory of another State which would, in any event, have no simple route of stopping or reversing it. Thus, it is perhaps not surprising that customary international law has been highly permissive on this front. The starting point is the judgment of the Permanent Court of International Justice (PCIJ) in *Lotus* (1927)[21] where a French and a Turkish steamer collided on the high seas resulting in the death of eight Turkish sailors and passengers. The issue was whether Turkey could institute criminal proceedings against a French lieutenant for his acts on the French ship, based on the effects of those acts on the Turkish steamer which international law treats as an extension of Turkish territory. The PCIJ commented on the ambit of the territoriality principle, and on jurisdictional discretion of States more generally:

> It does not, however, follow that international law prohibits a State from exercising jurisdiction in its own territory, in respect of any case which relates to acts which have taken place abroad, and in which it cannot rely on some permissive rule of international law. Such a view would only be tenable if international law contained a general prohibition to States to extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, and if, as an exception to this general prohibition, it allowed States to do so in certain specific cases. But this is certainly not the case under international law as it stands at present. Far from laying down a general prohibition to the effect that States may not extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, it leaves them in this respect a wide measure of discretion, which is only limited in certain cases by prohibitive rules; as regards other cases, every State remains free to adopt the principles which it regards as best and most suitable. This discretion left to States by international law explains the great variety of rules which they have been able to adopt without objections or complaints on the part of other States… In these circumstances all that can be required of a State is that it should not overstep the limits which international law places upon its jurisdiction; within these limits, its title to exercise jurisdiction rests in its sovereignty.[22]

The approach that 'everything that is not prohibited is permitted' (as opposed to 'everything that is not permitted is prohibited') is pervasive in the domestic legal sphere, but has met with

---

[21] *The Case of the SS "Lotus" (France v Turkey)* (1927) PCIJ Reports, Series A, No 10.
[22] Ibid., para 46 *f* [emphasis added].

stiff opposition at the international level.[23] Yet, arguably it has been endorsed, albeit in a different context, by the International Court of Justice in its Advisory Opinion on the *Declaration of Independence of Kosovo* (2010)[24] when it concluded that it only needed to establish whether 'international law prohibited the declaration'.[25] This permissive stance means that for legislative jurisdiction the principles, in particular the territoriality principle, have virtually no restrictive force, allowing States to make regulatory assertions as and when they desire.

The main restriction then comes as a matter of real-politic, rather than law – States are, by definition, not interested in regulating matters that have *no link* with their territory or population. In that sense, jurisdictional principles may be understood as evidencing when States have manifested a regulatory interest. A second, much weaker restriction derives from the objectives that lie behind the grand design of the global patchwork of States whereby each exercises regulatory control over its 'patch' or territory. So the very concept of territorial statehood entails the *sharing* of control between States and, arguably by implication, the fair treatment of individuals, protecting them from unreasonable compounding or conflicting obligations. Although the concurrency of an individual's obligations arising from multiple States is inevitable in a world of global communications, travel and trade, such concurrency becomes problematic the higher the number of States that claim regulatory competence in parallel – a problem endemic in the online context. Brierly, in 1928, noted: 'The suggestion that every individual is or may be subject to the laws of every State at all times and in all places is intolerable.'[26] For this reason, one may argue that the strength of any link of a State with a to-be-regulated transnational (online) event ought to be measured against potentially competing links by other States. A link with an event that is so weak that it could also be relied upon by innumerable other or indeed all States – again as is often the case for online events – is intolerable in all but the rarest circumstances.

A related question is whether public international law on jurisdiction also governs civil matters. Does it impose limits on private international law, or are the jurisdictional rules solely concerned with criminal jurisdiction? Akehurst in his seminal article on 'Jurisdiction in International Law' in the early 1970s argued for the non-application of international law to civil disputes:

> Of course, rejection of analogies drawn from criminal trials does not necessarily mean that international law imposes no limitation whatever on jurisdiction in civil cases – the limitations might simply be of a different kind. But … when one examines the practice of States … one finds that States claim jurisdiction over all sorts of cases and parties having no real connection with them and that this practice has seldom if ever given rise to diplomatic protests.[27]

---

[23] Vaughan Lowe and Christopher Staker, 'Jurisdiction' in Malcolm D Evans (ed), *International Law* (OUP 2010) 313, 318 *ff*. See also Ryngaert (n 17) 36 *ff*, for more general commentary.

[24] *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo* (ICJ Advisory Opinion) 22 July 2010, http://www.icj-cij.org/docket/files/141/15987.pdf.

[25] Ibid., para 56.

[26] James L Brierly, 'The "Lotus' Case" (1928) 44 *Law Quarterly Review* 154, 161.

[27] Akehurst (n 18) 170 [emphasis in the original, internal citations omitted]. See also Gerald Fitzmaurice, 'The General Principles of International Law' (1970) 92 *Recueil Des Cours* 1, 218; Gerfried Mutz, 'Private International Law' in Rudolph Bernhardt (ed), *Encyclopaedia of Public International Law* (1987) Vol 10, 330, 334; Malcolm Shaw, *International Law* (CUP 2008) 652.

There are numerous cases that imply the continued validity of Akehurst's analysis.[28] However, there are also academics who have asserted the contrary;[29] and there are also those civil cases, such as US anti-trust treble-damages-awards cases and recent Alien Tort Statute litigation, that triggered protests (as an indicator of illegality[30]) against undue extraterritoriality from other States.[31] Given the general permissiveness of international law on legislative jurisdiction, it seems that it would make little, if any, practical difference whether international law imposed limits on private international law or not. The civil cases that triggered strong protests and allegations of extraterritoriality suggest that it is not the civil or criminal nature of the regulatory activity per se that may explain the protest, but rather the (economic) repercussions flowing from the extraterritorial assertion. In the US anti-trust treble-damages-awards cases and recent Alien Tort Statute litigation, the crux was that European economic interests stood to suffer significantly. On this basis, the discussion here does not draw a strong division between civil and criminal transnational regulation, but shows the common themes running through them. In any event, the civil-criminal division is often blurred, particularly for those obligations (e.g., data protection or copyright) that are 'civil' in so far as they govern the relationship between private parties, but are also enforced by public regulatory authorities through the imposition of criminal or administrative sanctions.[32]

Restrictive on Enforcement Jurisdiction

As permissive as customary international law is on assertions of legislative jurisdiction, as restrictive it is in respect of enforcement jurisdiction. Thus, whilst States can make far-reaching regulatory assertions over foreign activity and foreign actors as a matter of principle, they cannot take actions to enforce them over and beyond their territorial boundaries. Again the PCIJ in *Lotus*[33] stated customary international law when it drew a clear division between enforcement and legislative jurisdiction:

> the first and foremost restriction imposed by international law upon a State is that … it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial … It does not however, follow that international law prohibits a State from exercising jurisdiction in its own territory, in respect of any case which relates to acts which have taken place

---

[28] In the UK, *Kuwait Airways Corp v Iraqi Airways Co* [2002] 3 All ER 209, the House of Lords decided that it had jurisdiction, and would exercise it, in respect of a claim between two foreign parties concerning a conversion that took place entirely abroad: 'it is an action in tort which has nothing whatever to do with England save that England has made itself available as the forum for litigation' (Lord Scott of Foscote para 174); see also *Berezovsky v Michaels and Others* [2000] UKHL 25 or *The Vishva Ajay* [1989] 2 Lloyd's Rep 558.

[29] F A Mann, 'The Doctrine of Jurisdiction in International Law' (1964) 111 *Recueil Des Cours* 1, 73 *ff*; F A Mann, 'The Doctrine of International Jurisdiction Revisited after Twenty Years' (1984) 186 *Recueil Des Cours* 9, 20 *ff*, 67 *ff*; Ian Brownlie, *Principles of Public International Law* (OUP 2001) 302.

[30] Ryngaert (n 17).

[31] See in particular the Amicus Briefs submitted in the US Supreme Court Judgment in *Kiobel v Royal Dutch Petroleum Co* 569 US (17 April 2013), affirmed 621 F3d 111 (2d Cir 2010).

[32] See, e.g., the criminal copyright case of *Donner (Free movement of goods)* [2012] EUECJ C-5/11 (21 June 2012); or Bogdan, 'Google was fined by French and Spanish Data Protection Authorities' (15 January 2014) EDRi (European Digital Rights), http://edri.org/google-fined-french-spanish-data-protection-authorities/.

[33] *Lotus* (n 21).

> abroad … Such a view would only be tenable if international law contained a general prohibition to States to extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory … But this is certainly not the case under international law as it stands at present.[34]

Enforcement jurisdiction is strictly territorial; a State can never enforce its law on the territory of another State, e.g., by sending its police officers there (except with the consent of the other State). As Lombois put it:

> The law may very well decide to cast its shadow beyond its borders; the judge may well have a voice so loud that, speaking in his house, his condemnations are heard outside; the reach of the police officer is only as long as his arm … he is a constable only at home.[35]

The restrictiveness of enforcement jurisdiction is one manifestation and implementation of the principle of non-intervention that protects the territorial sovereignty of States by prohibiting physical or coercive interferences by other States.[36] Although customary international law on enforcement jurisdiction has thus – quite unlike the principles of legislative jurisdiction – clear restrictive force, its apparent simplicity is misleading. Interferences with a State's territory fall along a spectrum of relative tangibility and severity, and not all are captured by the prohibition.[37] Certainly, legally requested data transfers by global online platforms are a case in point and contention (discussed below). Overall, the mismatch between the wide reach of legislative jurisdiction and the strict territoriality of enforcement jurisdiction creates an enforcement gap, that initially made itself strongly felt in the online context, but has increasingly been filled with the cooperation of platforms and other intermediaries through which much transnational activity can be filtered.

As final preliminary comments, it is worth bearing in mind, *first*, that 'jurisdiction' provides the legal instrumentality through which a political community implements its peculiar vision of the good life. Jurisdictional wranglings reflect each State's desire to uphold their legal standards on their territories as to what is good, just and fair, and these standards vary across a wide spectrum of regulatory concerns. Sovereignty, as realised by jurisdiction, allows for a multitude of political communities to agree to disagree on the parameters of the good life. In many cases discussed below, the activity complained about was tolerated, and not illegal, and at times perfectly legitimate, in the place where it was hosted, and yet illegal in the place(s) where it was accessed. Some high-profile cases have made the headlines, such as the blocking

---

[34] Ibid., 18.

[35] Claude Lombois, *Droit Penal International* (Daloz 1979) 536, cited in Pierre Trudel, 'Jurisdiction over the Internet: A Canadian Perspective' (1998) 32 *The International Lawyer* 1027, 1047.

[36] For an early multilateral statement, see Art 8 of Montevideo Convention on the Rights and Duties of States (26 December 1933, 49 Stat. 3097, T.S. 881): '[n]o state has the right to intervene in the internal or external affairs of another'.

[37] *Nicaragua v United States of America (Military and Paramilitary Activities in and against Nicaragua)* [1986] ICJ Rep 14, para 245, holding that a trade embargo was not 'coercive' so as to breach the prohibition of non-intervention. See also Jens David Ohlin, 'Did Russian Cyber-Interference in the 2016 Election violate International Law' (2017) 95 *Texas Law Review* 1579 and Sean Watts, 'Low-intensity Cyber Operations and the Principle of Non-intervention' in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds), *Cyber War: Law and Ethics of Virtual Conflicts* (OUP 2015).

of 'The Innocence of Muslims' video by YouTube in Egypt and Libya[38] or the wholesale blocking of foreign political material in China, and these incidents are decried as intolerable censorship by repressive political regimes. Yet, in principle these States do little more than liberal democracies that also routinely monitor and repress content considered 'unacceptable' under *their* legal standards. The difference lies in what is seen as unacceptable; they are all equally motivated by the desire to protect their territory from foreign-based online activities that undermine their local laws, and implicitly moral and political values.[39] Whilst from a jurisdictional perspective, the subject-matter of the law, as opposed to its purported territorial reach, is generally of no further concern, it *is* useful to remind oneself that sovereignty, and implicitly jurisdiction, seek to protect the self-determination of a people and legal diversity across the globe. In the words of Martti Koskenniemi:

> Today, it [sovereignty] stands as an obscure representative against disillusionment with global power and expert rule … [and] points to the possibility, however limited or idealistic, that whatever comes to happen, one is not just a pawn in other people's games but, for better or for worse, the master of one's own fate.[40]

Second, 'jurisdiction' also provides a legal instrumentality to protect national economic interests, e.g., by trying to protect the local market from foreign competitors especially, but not only, where they do not provide goods or services on a level playing field, or from online actors who extract valuable data from local consumers without benefiting the local economy. In short, jurisdiction, or regulatory competence, in the transnational context is underwritten by strong political and economic drivers that go to the heart of statehood and sovereignty.

3. ADJUDICATIVE OR LEGISLATIVE JURISDICTION ON THE INTERNET

In 1996 Johnson and Post argued in their seminal article 'Law and Borders – The Rise of Law in Cyberspace'[41] that laws based on geographical location were not tenable on the internet as all online activity is as much located in one State as in another and therefore no one State had a greater entitlement than any other State to regulate any particular online activity. This, in turn, undermined each State's claim to do so. Any attempt by a State to apply their law to the internet, particularly online activity originating from abroad, would raise problems of

---

[38] CNN, 'Death, destruction in Pakistan amid protest tied to anti-Islam film', *CNN* (21 September 2012) https://edition.cnn.com/2012/09/21/world/anti-islam-film-protests/index.html; Peter Hervik, 'The Danish Muhammad Cartoon Conflict' (2012) No 13 *Current Themes in IMER Research*, http://www.mah.se/upload/Forskningscentrum/MIM/CT/CT%2013.pdf.

[39] See discussion of online gambling or trademark disputes. Adam Liptak, 'A Wave of the Watch List, and Speech Disappears', *New York Times* (4 March 2008) https://www.nytimes.com/2008/03/04/us/04bar.html, noting the blacklisting of domain names occurs under the Trading with the Enemy Act 1917, through a blacklist established by the Office of Foreign Assets Contract (OFAC) and passed onto US domain name registrars.

[40] Martti Koskenniemi, 'Conclusion: Vocabularies of Sovereignty – Powers of a Paradox' in Hent Kalmo and Quentin Skinner (eds), *Sovereignty in Fragments* (CUP 2010) 222, 242.

[41] David R Johnson, David G Post, 'Law and Borders – The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367.

democratic legitimacy, fairness to the individual and enforceability. In many respects Johnson and Post were entirely correct and yet, States have consistently asserted their right to regulate online activity from within or from outside. The link they have relied upon has invariably been a territorial link between the online activity and the State: the site in question can be, or has been, accessed from the State's territory, even if its author or server is abroad.[42]

The Destination Approach: Accessibility versus Targeting

The following provide judicial and legislative examples of regulatory assertions made by States over foreign actors and their activities, organised by broad harm categories.[43] Although the examples are varied in content and type, they have in common that the assertions are always based on the *effect* or *impact* of the foreign activity on local soil. The disagreement amongst these cases is how strongly that effect must be felt: is it sufficient harm that the site was accessible from the territory, or must it be shown that it was objectively intended for local users in particular and has a substantial effect on the territory? The difference comes down to whether Brierly's warning is heeded or not, namely, that it would be 'intolerable' for an individual (or corporation) to be subjected 'to the laws of every State at all times and in all places.'

Local harm: moral and political values

Content regulation that targets hate speech or obscene or defamatory speech gave rise to the early internet jurisdiction cases, frequently to loud outcries from academic, political and commercial communities. Typically, in the French case of *LICRA & UEJF v Yahoo! Inc & Yahoo France* (2000)[44] Yahoo! Inc was subjected to France's prohibition on the distribution of Nazi-memorabilia[45] in respect of its auction site where third parties sold Nazi artefacts, which could be accessed from French soil and bought by French consumers. The justification for France's jurisdiction over yahoo.com was – in the words of the court – that the 'harm was suffered on the territory of France' simply by virtue of the site's accessibility in France. As Yahoo! Inc could with 70 per cent accuracy determine the location of its users, the court ordered the site to be made inaccessible from French soil, and thereby leave it intact in the rest of the world. Notably, the case was a civil-criminal hybrid as the civil action was based on a manifest breach of criminal law. The case also foreshadows key themes that emerged later within the field. First, the judgment made clear that France will not tolerate the watering down of its legal standards by online activities that originate from other States that legally tolerated such content, most prominently the US. Second, the case shows the contestability of the level

---

[42] See below.

[43] These are not comprehensive, with 'security' being a notable omission.

[44] *LICRA v Yahoo! Inc & Yahoo France* (Tribunal de Grande Instance de Paris, 22 May 2000), affirmed in *LICRA & UEJF v Yahoo! Inc & Yahoo France* (Tribunal de Grande Instance de Paris, 20 November 2000). An even earlier case was the German *CompuServe* (1995) where German police raided *CompuServe*'s German offices in an investigation concerning online pornography and CompuServe responded by temporarily suspending all of its 200 plus newsgroups (hosted in the US and accessible worldwide) for its 4 million users because it was technically incapable of blocking only Germans. Later its local manager, Felix Somm, was convicted under German obscenity laws and received a two-year suspended sentence; overturned on appeal as there was no blocking technology available to CompuServe: *R v Somm* Amtsgericht München (17 November 1999).

[45] Arts 808 and 809 of the New Code of Civil Procedure.

of local harm needed to justify a regulatory assertion by a destination or host State. In this case, Yahoo! Inc run the yahoo.com site (hosted in the US, in English, primarily for a US audience) and a yahoo.fr site (hosted in France for the French market and compliant with French law). Yet, this latter site did not relieve Yahoo! Inc of accountability under French law in respect of the former site, as even yahoo.com was accessible in France. Third, the claimants targeted a platform, as opposed to the primary wrongdoers, here the sellers on the auction website in the expectation that these large platforms with large markets in Europe will, after all, comply with the regulatory demands made by their 'host' States,[46] and thus become intermediaries to oversee whole speech environments. Cases of a similar kind followed in other jurisdictions and legal contexts, see below, and normalised the *Yahoo* ruling.[47]

As online hate speech of a wide variety originating from within and outwith territorial borders has crystallised as a key regulatory concern, platforms have become a new regulatory target. The first State to formalise content responsibilities of platforms has been Germany through its *Network Enforcement Law* (2017).[48] The law requires social media platforms to remove hate speech, fake news and other illegal content upon notice by users – generally within 24 hours (for obviously illegal material) and within seven days (for all other illegal material), backed by a fine of up to €50 million,[49] and amended in 2020 to require platforms to notify the Federal Police immediately of alleged criminal content.[50] Jurisdictionally, the law's approach is unusual as it attaches takedown duties only to large platforms, that is, those with more than two million users in Germany.[51] In contrast to the *Yahoo* judgment which effectively exposed any foreign site, regardless of its user numbers in France, to French content prohibitions, the German law makes a substantial harm potential within the territory a prerequisite for its application. It thereby seeks to strike a balance between the level of harm suffered within the territory, the legal burden on foreign (intermediary) actors and its own enforcement capacities. Although a similar law in France was struck down by the French Constitutional Court in 2020 on the basis that 'illicit content' was too vague a concept to allow platforms to make measured decisions within a short timeframe and effectively encourages them to remove too much content,[52] there has been a sustained drive at EU and Member State level to co-opt large digital platforms into gatekeeping responsibilities, albeit so far via soft law obligations.[53]

---

[46] Uta Kohl, *Jurisdiction and the Internet* (CUP 2007) Chapter 6.

[47] *R v Töben* BGH (12 December 2000) 1 StR 184/00, LG Mannheim; (2001) 8 *Neue Juristische Wochenschrift* 624.

[48] Gesetz zur Verbesserung der Rechtsdurchsetzung in Sozialen Netzwerken (1 Sept 2017, BGBl I S 3352).

[49] Section 3(2), 4.

[50] Natasha Lomas, 'Germany Tightens Online Hate Speech Rules to Make Platforms Send Reports Straight to the Feds', *Techcrunch* (19 June 2020).

[51] Section 1(2).

[52] Décision No. 2020-801 DC du 18 juin 2020 (18 June 2020, Constitutional Court) https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm.

[53] European Commission, *The Code of conduct countering illegal hate speech online* (31 May 2016, together with four major IT companies: Facebook, Microsoft, Twitter and YouTube) https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.

In the same vein, the UK *Online Harms White Paper* (2019)[54] proposes a statutory duty of care for platforms and other intermediaries to protect users from harmful content, with harmful being expansively defined to include the whole spectrum of conceivable harms.[55] Unlike the German Network Law, the *White Paper* envisages the application of this duty to reach a wide range of online providers, including companies outside the territory 'that *provide services to UK users*. We will design the regulator's powers to ensure that it can take action against companies without a legal presence in the UK, including blocking platforms from being accessible in the UK as a last resort'.[56] Thus, although the duty is designed to work flexibly in line with the nature of the online provider, the legitimating link for territorial competence is as weak as it was in *Yahoo*; the duty attaches to any foreign provider no matter how large or negligible their effect on UK territory. Of course, in situations of negligible impact it is unlikely that any enforcement action e.g., blocking, would be taken, but this argument substitutes real-politic for a measured law with a focused restraint in its extraterritorial application. Jurisdictionally, the *White Paper's* approach is in line with the English case of *R v Perrin* (2002),[57] where a French director of a US company operating a US hosted website was convicted of the offence of publishing an obscene article contrary to UK Obscene Publications Act 1959 in relation to the freely accessible preview site of his pornography subscription site – simply because the site was accessible in England, without any evidence whether it had in fact been accessed and how much.[58] Yet, the case concerned a primary wrongdoer, whilst the framework proposed by *White Paper* is mainly directed at intermediaries who are at best secondary wrongdoers which arguably further weakens the legitimacy of the strict territorial application regardless of the actual or intended territorial effect.

The above instances deal with online content unacceptable from a public law perspective of the relevant State; but jurisdictional issues have also arisen where individuals have alleged individual harm from an online publication, typically in transnational defamation disputes. Here one might have expected that the judiciary would strike the balance between not overburdening providers with too many concurrent obligations under multiple national laws *and* preserving the integrity of the national law space, more in favour of the former. This, however, has not been the case. In the Australian case of *Dow Jones & Co Inc v Gutnick* (2002)[59] where the court held Barrons Online, a subscription site by US publisher for a mainly US audience and an insignificant Australian readership, was liable under Australian defamation law, simply because the claimant enjoyed a reputation in Australia, and must be presumed to have suffered harm there. The same approach was endorsed in the English case of *Harrods Ltd v Dow Jones*

---

[54] Department for Digital, Culture, Media & Sport, Home Office, *Online Harms White Paper* (8 April 2019, CP59).

[55] Ibid., para 2.2, including child sexual exploitation, terrorist content, modern slavery, pornography, content encouraging suicide, incident of violence, sale of illegal goods, cyberbullying, intimidation, disinformation etc.

[56] Ibid., para 6.9 [emphasis added].

[57] *R v Perrin* [2002] EWCA Crim 747. Perrin's application to the European Court of Human Rights, arguing that the UK regulation breached his right to freedom of expression, was rejected: *Perrin v UK* (ECHR 18 October 2005, No 5446/03).

[58] Although Perrin was a resident in the UK at the time of wrongdoing, the court did not focus on that fact although no doubt it fed into the decision to go ahead with the prosecution. It appears that – as a matter of establishing personal responsibility of the site – Perrin admitted being a director and majority shareholder of one or more US companies involved in operating the website from the US.

[59] [2002] HCA 56, which affirmed *Gutnick v Dow Jones & Co Inc* [2001] VSC 305.

Co Inc (2003)[60] concerning Harrods Ltd's defamation claim, again against Dow Jones. The offending article, which appeared only in the US edition of the journal, not the European one, had been sent to ten subscribers of the US edition in the UK and there were a few hits on the online edition, in contrast to its US circulation of 1.8 million copies. As the claim was restricted to the damage arising from UK subscriptions, the court allowed it to proceed in England, as if this somehow would make the regulatory burden on the publisher proportionate to the level of harm of the publication. Still, these judgments have been followed by later ones where again the limited harm potential of a very small local readership of a foreign publication, invariably by a US provider, did not stop the invocation of local defamation standards.[61] In response, the *UK Defamation Act* 2013 has now introduced a highly restrained jurisdictional approach, whereby an English court will only hear a claim against a foreign publisher, if it 'is satisfied that, of all the places in which the statement complained of has been published, England and Wales is clearly the most appropriate place in which to bring an action in respect of the statement'.[62] This is wholly exceptional for defamation law; it appears to be designed to stop the parcelling off of a global defamatory publication into discrete national actions, and imports a comparative inquiry whereby the relative link of the action with England and Wales is compared with those with other States. Perhaps not coincidentally, the Act also makes claims against platforms and other intermediaries, as secondary wrongdoers, a remedy of last resort.[63] This and the jurisdictional restraint may be understood as a recalibrated framework of defamation law in response to the online environment with its much-heightened level of public speech and transnationality. It also, after all, suggests that States may be more ready to sacrifice remedies for individual harm in the global context than for comparable public harms.

Local harm: economic interests

Not all online jurisdictional disputes are explicable with reference to varying moral or political values – as is the case in respect of the prohibitions on, and definitions of, hate or other harmful speech crimes and defamation standards. Especially in commercial contexts, there may be large-scale global consensus on legal standards as, e.g., in respect of intellectual property, and even if there is no such consensus, the jurisdiction disputes may not be driven primarily by a desire to preserve the national law space as such; rather, it provides for an avenue to protect local market players from foreign competition. In those instances, jurisdictional claims by States have often invoked accusations of illegitimate protectionism.

Online gambling is a case in point. Gambling is a lucrative industry; more precisely it is lucrative for the State in which the provider is established through the creation of employment and as a source of revenue. These benefits are lost if the gambling services are provided by a foreign operator who may undermine, and certainly competes with, the local gambling industry, whilst leaving the State to deal with the social and economic problems flowing from gambling addictions. As foreign providers offer none of the economic advantages associated

---

[60] [2003] EWHC 1162 (QB). In *Dow Jones & Co v Harrods Ltd* 237 F Supp 2d 394, the New York District Court refused to grant to Dow Jones a declaratory judgment and an injunction requiring Harrods Ltd to abstain from pursuing a defamation claim in the UK.

[61] *Lewis & Ors v King* [2004] EWCA Civ 1329; *McGrath & Anor v Dawkins & Ors* [2012] EWHC B3 (QB). *Persönlichkeitsverletzungen durch ausländische Internetveröffentlichungen* (2 March 2010 BGH Az. VI ZR 23/09).

[62] Section 9(2).

[63] Section 10.

with gambling activity and all of its disadvantages, they have been subject to regulatory hostility and aggressive jurisdictional responses by most States. In respect of the US attitude, where online gambling is largely prohibited, one commentator succinctly noted:

> The fairly harsh approach to online gambling is a reversal of both the federal government's … receptivity to tribal gaming, and its acceptance of the recent liberalization of gambling laws in most U.S. states. The fierceness … in this area is puzzling until one realises the one factor at stake in … traditional gambling, but not at stake in Internet gambling: Money. … Internet gambling, hosted by foreign operators, not only generates zero governmental revenue and zero jobs, it also threatens traditional gambling.[64]

Thus even in the absence of national differences to gambling activities, there would be significant jurisdictional tensions simply because of the economic disadvantages of competing foreign providers. These tensions have manifested themselves widely. For example, a Dutch court in *National Sporttotaliser Foundation v Ladbrokes Ltd* (2003)[65] ordered the defendant, Ladbrokes, based in England and Gibraltar, to make its gambling site inaccessible to Dutch residents as it did not comply with Dutch licensing requirements. Australia largely prohibits any local or foreign provider[66] from offering online gambling services to people in Australia by virtue of the *Interactive Gambling Act 2001 (Cth),* whilst local Australian providers are free to offer their gambling services to punters abroad.[67] The territorial touchstone is whether the provider 'has an *Australian-customer link* if, and only if, any or all of the customers of the service are physically present in Australia'.[68] Australia seeks to obtain the benefits derived from gambling services, without suffering its losses. In New Zealand the *Gambling Act 2003* prohibits outright 'remote interactive gambling',[69] but excludes from the definition 'gambling by a person in New Zealand conducted by a gambling operator located outside New Zealand'.[70] However, the reach of foreign providers is circumscribed by prohibiting local online and offline intermediaries (e.g., ISPs, local sites and offline publishers) from advertising foreign gambling services in New Zealand.[71] Instead of seeking to control local gambling through prohibitions on foreign gambling providers which are difficult to enforce, New Zealand targets local intermediaries (that provide knowledge of, and access to, the foreign services) over which full enforcement power is present.

That jurisdictional claims over online gambling are far more centred on economic interests than varying moral values is illustrated by two disputes that have brought online gambling

---

[64] Christine Hurt, 'Regulating Public Morals and Private Markets: Online Securities Trading, Internet Gambling and the Speculation Paradox' (2005) 86 *Boston University Law Review* 371, 375 *f.*

[65] District Court, The Hague (27 January 2003), see also *Holland Casino v Paramount Holdings et al* District Court, Utrecht (27 February 2003). For a comparable German judgment, see *Unzulässiges Online-Glücksspielangebot* OLG Hamburg (19 August 2004) 5 U 32/04, (2004) 12 *Computer und Recht* 925; following *Schöner Wetten* BGH (1 April 2004) I ZR 317/01.

[66] Section 14 of the Interactive Gambling Act 2001 (Cth): 'this Act extends to acts, omissions, matters and things outside Australia'.

[67] Sections 8, 15 (unless the foreign country has been declared a 'designated country' see ss.15A, 9A, 9B).

[68] Section 8, see also s.8F inserted by the Interactive Gambling Amendment Act 2017 for an expanded definition of 'prohibited internet gambling content'.

[69] Section 9(2)(b) and 19 of the Gambling Act 2003.

[70] Section 4 of the Gambling Act 2003 on the definition of 'remote interactive gambling'.

[71] Section 16 of the Gambling Act 2003.

restrictions into conflicts with trade agreements, at the EU and WTO level respectively. In both cases, the attempt by one State to restrict foreign online gambling services was challenged as being inconsistent with trade commitments.[72] In *Gambelli* (2003)[73] the European Court of Justice was presented with a challenge to Italy's attempt to impose criminal sanctions on Italian agencies which, contrary to local licensing requirements, acted as online intermediaries for the UK bookmaker Stanley International Betting Ltd. Effectively, Italy wanted to protect its very lucrative national monopoly in the sports betting and gaming sector. This protectionist policy was successfully challenged as contrary to the freedom of establishment and freedom to provide services of foreign providers (now Art 49 and 56 of the Treaty on the Functioning of the EU). These freedoms demanded that Member States take a regulatory hands-off approach to gambling providers from other Member States and regulated by those other State, unless the regulation was justifiable 'for reasons of overriding general interest', e.g., to reduce the gambling, but not out of a fear of losing revenue. Similarly, the WTO Appellate Body was presented with the same type of conflict in *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services* (2005).[74] Antigua and Barbuda lodged a complaint against the US with the WTO in 2003, alleging that the US prohibition on the cross-border supply of gambling and betting services was inconsistent with 'market access' commitments made by the US under Article 16 of the *General Agreement on Trade in Services* (GATS). Antigua blamed the increasingly aggressive US strategy (enforced with the help of local US intermediaries) towards the operation of cross-border gaming activities in Antigua for the significant decline of gambling operators in Antigua: 'from a high of up to 119 licensed operators, employing around 3,000 and accounting for around ten per cent of GDP in 1999, by 2003 the number of operators has declined to 28, employing fewer than 500'.[75] The WTO Appellate

---

[72] In the EU gambling was specifically excluded from the Electronic Commerce Directive and in particular the Directive's origin rule (i.e., that online service providers should only be regulated by their home State). Recital 16 and Art 1(5)(d) of the Electronic Commerce Directive.

[73] *Criminal Proceedings against Piergiorgio Gambelli* C-243/01 [2003] ECR I-13031. In *Criminal Proceedings against Massimiliano Placanica and Others C-338/04, C-359/04 and C-360/04* [2007] ECJ ECR I-0000 it was again held that Italy's licencing regime which excluded companies listed on a stock exchange from tendering for a betting licence violated the freedom of establishment and the freedom to provide services as it went beyond what is necessary to achieve the objective of preventing the exploitation of the industry for criminal proposes. See Hörnle (n 1) Chapter 4; see also Katherine A Lovejoy, 'A Busted Flush: Regulation of Online Gambling in the European Union' (2014) 37 *Fordham International Law Journal* 1526.

[74] *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services* first heard by the WTO Dispute Settlement Panel (WTO Panel, 10 November 2004, WT/DS285/R) and then by the Appellate Body (WTO Appellate Body, 7 April 2005, WT/DS285/AB/R). In 2007 the WTO panel concluded 'that the United has failed to comply with the recommendations and rulings of the DSB in this dispute' (WTO Panel, 30 March 2007, WT/DS285/RW) which paved the way for a compensation claim and then trade sanction by Antigua. http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm.

[75] *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services* (WTO Panel, 10 November 2004, WT/DS285/R) para 3.5. A similar complaint against the US was lodged in 2007 by the Remote Gambling Association with the European Commission which came to very similar conclusion as WTO Panel. European Commission, *Report to the Trade Barriers Regulation Committee: Examination Procedure concerning an Obstacle to Trade, within the Meaning of Council Regulation (EC) No 3286/94, consisting of Measures Adopted by the United States of America Affecting Trade in Remote Gambling Services* (Brussels, 10 June 2009).

Body rejected the US claim that by excluding sporting services from its GATS commitments, it had also excluded gambling and betting services, and held that various US Acts were inconsistent with its GATS commitments. As in *Gambelli*, the Appellate Body held that 'public moral' or 'public order' may exceptionally justify market access barriers, provided there were no other reasonable alternative measures. Given that the US had exempted domestic providers from the very prohibitions it sought to apply to foreign operators, it could not rely on these exceptions. Online gambling activity shows how jurisdictional claims by States over foreign online providers based on its effect on the local territory may serve to protect local economic interests, and thus may rightly come into conflict with free trade commitments, whether at the global or regional level.

A more recent manifestation of transnational jurisdiction asserted in the economic domain is provided by Germany's implementation of the Fifth Anti-Money Laundering Directive,[76] which makes foreign cryptocurrency providers – like any providers of banking and financial services – subject to the German regulatory regime, if they have actively solicited customers in Germany, but not if they simply offer services to German customers who have responded to general internet offerings (reverse solicitation).[77] This presents a classic instantiation of the targeting approach to jurisdiction whereby a State regulates only those online providers that have, or are likely to have, a real impact on its territory. The virtue of this approach lies in striking a proportionate balance between the harm potential, on the one hand, and law enforcement efforts and regulatory burden on online providers, on the other hand. This makes it a measured option even, or perhaps especially, in criminal and regulatory contexts.

In parallel to jurisdiction vis-à-vis harmful content, the judiciary has also been strongly defensive of local claimants in civil commercial claims – irrespective of the negligible impact of the foreign conduct within the jurisdiction. Thus, in *Pinckney v KDG Mediatech* (2013)[78] the CJEU held that copyright claims fell under the tort head in Article 5(3) of the Jurisdiction Regulation,[79] which:

> does not require … that the activity concerned to be 'directed to' the Member State in which the court seised is situated … [Jurisdiction is established] if the Member State in which that court is situated protects the copyrights relied on by the plaintiff and the harmful event alleged *may* occur within the jurisdiction of court seised.[80]

Similarly, in *Wintersteiger v Products 4U Sondermaschinenbau GmbH* (2012)[81] the CJEU upheld an Austrian court's jurisdiction to hear a trademark claim based on an Austrian trade-

---

[76] (Fifth) Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending (Fourth) Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU; implemented in Germany by Gesetz zur Umsetzung der Änderungs–richt–linie zur Vierten EU-Geldwäscherichtlinie (BGBl IS 2602 Nr50); 12 Dec 2019, in force since 1 January 2020.

[77] Manuel Lorenz, 'Germany's Approach to Crypto-assets and their Safeguarding under 5MLD and Financial Regulation' (27 February 2020, *Baker & McKenzie, Global Compliance News*).

[78] *Peter Pinckney v KDG Mediatech AG C-170/12* [2013] EUECJ (3 October 2013).

[79] Now Art 7(2) of the Recast Brussels Regulation 1215/2012.

[80] *Peter Pinckney v KDG Mediatech AG* C-170/12 [2013] EUECJ (3 October 2013) paras 42 and 43 [emphasis added].

[81] *Wintersteiger v Products 4U Sondermaschinenbau GmbH* C-523/10 [2012] ECR I-0000; see also *Joined Cases eDate Advertising and Martinez* C-509/09 and C-161/10 [2011] ECR I-10269.

mark, where the allegedly infringing advertising had solely occurred on google.de and not google.at and the claimant held no registered trademark in Germany. Still, Austria, as the place of registration, was considered to be best suited to hear the claim.[82] The possibility of an alternative approach was opened up by the Advocate General who argued for a more substantial effect of the activity within the territory as a basis for the court's jurisdiction:

> The fundamental factor or point is whether the information disseminated on the internet is really likely to have an effect in the territory where the trade mark is registered. *It is not sufficient if the content of the information leads to a risk of infringement of the trade mark* and instead it must be established that there are objective elements which enable the identification of conduct which is in itself intended to have an extraterritorial dimension. For those purposes, a number of criteria may be useful, such as the language in which the information is expressed, the accessibility of the information, and whether the defendant has a commercial presence on the market on which the national mark is protected.[83]

Despite the endorsement of this 'targeting' approach in some intellectual property cases, as, e.g., in *L'Oréal SA and Others v eBay International AG and Others* (2011),[84] the clearest adoption yet of a moderate approach that looks for more than a negligible effect on the local market has yet again come in legislative form. Under Article 17(1)(c) of the Recast Brussels Regulation,[85] a consumer only gets the benefit of the protective provision (i.e., bringing the action in their home jurisdiction) if the foreign online activities (that gave rise to the disputed consumer contract) were 'directed' at the consumer's jurisdiction; in *Pammer and Hotel Alpenhof* (2010)[86] the CJEU held that 'directing' is not satisfied simply by virtue of the site being accessible in the consumer's jurisdiction; a greater actual or intended effect was needed.

Local harm: informational privacy

The archetypal harms created by network society are data-related, and here personal data has emerged as a particularly valuable and sensitive category. Control of personal data carries repercussions both in economic terms (personal data is a valuable commodity) and in moral and political terms (personal data is an important extension of personhood and critical to personal autonomy in social, commercial and political spheres) – as broadly reflected in the

---

[82] *Wintersteiger v Products 4U Sondermaschinenbau GmbH* C-523/10 [2012] ECR I-0000, para 27, 28.

[83] *Wintersteiger v Products 4U Sondermaschinenbau GmbH* C-523/10 [2012] Opinion of the Advocate General ECR I-0000 paras 28–30 [internal marks omitted]. This moderate (targeting) approach to jurisdiction is, in theory, deeply embedded in the US jurisprudence on the 'due process' requirement under the Constitution Fifth and Fourteenth Amendment to the US Constitution, dealing with the right of 'due process' as against the Federal government and State governments respectively.

[84] *L'Oréal SA and Others v eBay International AG and Others C- 324/09* (2011) ECR I-6011, para 64, where the CJEU stated in respect of substantive trademark infringement: 'it must be made clear that the mere fact that a website is accessible from the territory covered by the trade mark is not a sufficient basis for concluding that the offers for sale displayed there are targeted at consumers in that territory'. See also *Football Dataco Ltd and Others v Sportradar GmbH and Another C-173/11* [2012] EUECJ, *Donner (Free movement of goods) C-5/11* [2012] EUECJ (21 June 2012), interpreting the Copyright Directive 2001/29/EC.

[85] Recast EU Regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (EC) No 1215/2012.

[86] Pammer *v Reederei Karl Schluter GmbH 8 Co KC* C-585/08 *and* Hotel Alpenhof *GmbH v Heller* C-144/09 [2010] ECR 1-12527.

right to informational privacy.[87] Transnational flows of personal data have thus given rise to significant jurisdictional clashes, partly because informational privacy is differently balanced against competing rights and public interests (e.g., freedom of expression or security) in different States, and partly because personal data is an economic (and security) asset over which States seek maximum control. These clashes in many ways epitomise the drivers underlying regulatory assertions over online activity more generally.

A key decision in this field has been the CJEU judgment in *Google Spain SL, Google Inc v AEPD* (2014)[88] on the right to be forgotten under the EU Data Protection Directive.[89] In this case, Mr González's professional activities as a lawyer were prejudiced by the fact that on a Google search of his name, the top result referred to an online edition of a Spanish newspaper of more than a decade before, with a notice of the forced sale of his property in attachment proceedings for the recovery of social security debts. Previously that information would only have been available upon visiting the archives of the newspaper, but with the internet it remained in the consciousness of his clientele. The overall question was whether Mr González had a 'right to be forgotten' under EU data protection law which would require Google to remove 'outdated' links from its search results, but this, in turn, depended in the first place on the EU data protection standards being applicable to the processing of search queries which occurred solely on US soil. The CJEU was quick to stretch Article 4 of the Directive to encompass search activities of Google as the 'operator of a search engine [that] sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which *orientates* its activity towards the inhabitants of that Member State'.[90] It makes sense for those US or other platforms that derive substantial financial gain from the data extracted from European customers to be subject to European data protection law, no matter where in the world they locate their processing activities. In a less ambiguous way, Article 3 of the GDPR, which has since replaced the Directive, extends its framework to the 'processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not'.[91] And even without such establishment, data controllers are subject to the Regulation where they extract personal data either whilst 'offering of goods or services, irrespective of whether a payment of the data subject is required, to … data subjects in the Union', or whilst 'monitoring … their behaviour as far as their behaviour takes place within the Union'.[92]

Although both *Google Spain* and Article 3 of the GDPR appear to adopt a targeting approach, neither comments on what exactly amounts to 'orientating' activity towards the EU,[93] or when may a business be said to 'offer goods and services' to consumers within the

---

87 For its most explicit recognition as a fundamental right, see Art 8 of EU Charter of Fundamental Rights. On cyberspace and human rights see Fidler (Ch 7 of this Handbook).

88 *Google Inc v Agencia Española de Protección de Datos, Mario Costeja González* C-131/12 (CJEU 13 May 2014); *Google Inc v Agencia Española de Protección de Datos, Mario Costeja González* C-131/12 (Opinion of Advocate General, 25 June 2013).

89 95/46/EC.

90 *Google Inc v Agencia Española de Protección de Datos, Mario Costeja González* C-131/12 (CJEU 13 May 2014) para 60; Art 4(1)(a) of the Directive. See also Art 29 Working Party, Opinion 1/2008.

91 Art 3(1) GDPR [emphasis added].

92 Art 3(2) GDPR.

93 Art 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgement on "Google Spain and Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12 (26 November 2014).

Union. Yet, for Google and other global platforms, this is vital for determining which of their platforms or activities must be made GDPR compliant. Thus, an important follow-up ruling by the CJEU came in *Google v CNIL* (2019) in which the Court decided that a 'right to be forgotten' takedown duty did neither extend to *all* google domains (as requested by the French Data Protection authority)[94] nor solely to the particular country-specific Google version that corresponds to the Member State from where the notice came.[95] Instead, de-referencing is required across all the versions corresponding to all the Member States,[96] considering that the new Regulation is designed to ensure 'a consistent and high level of protection throughout the European Union and to remove the obstacles to flows of personal data within the Union'.[97] Furthermore, the Court seemed to align itself with the Advocate General's Opinion that Google's knowledge of the territorial origin of searches (with a 99.94 per cent accuracy rating[98]) allows it to geo-block de-referenced search results from searches from within the EU, *regardless* of which country-specific Google version was used.[99] So a search through google.co.nz (New Zealand) used from French territory would appear to trigger Google's obligation to 'effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access… to the links which are the subject of that request'.[100] The holding is both deeply like and unlike the early *Yahoo* judgment. It is unlike it by attaching the main responsibility only, in the first place, to the domains that are clearly targeted at the Union i.e., not all search domains accessible in the Union must comply, but only those with corresponding domain names. However, *Google v CNIL* is exactly like *Yahoo* in respect of the residual duty to geo-block de-referenced search result whenever a search is carried out from Union territory. Both cases show the potentiality of an enhanced working of the territoriality principle in network society as implemented by platforms.[101] Their gatekeeping – enabled by close-up knowledge of users and their locations and enacted through encoded territorial borders – makes it rather difficult for Joe Bloggs to by-pass territorial law and order.

The destination approaches under customary international law

The question raised by the above is whether customary international law requires more than a negligible impact on the territory as the basis for a legitimate assertion of legislative or adjudicative jurisdiction. Since *Lotus* it has been explicitly recognised that in transnational wrongdoings, the State on the territory on which the wrong takes effect enjoys the right to regulate that conduct (objective territoriality principle[102]) alongside the State from where the

---

[94] Google v CNIL C-507/17 [2019] EU:C:2019:772 (CJEU, 24 Sept 2019) para 65, but see for exceptional circumstances, para 72.

[95] Ibid., para 66.

[96] Ibid., para 73.

[97] Ibid., para 66.

[98] Michele Finck, 'Google v CNIL: Defining the Territorial Scope of European Data Protection Law' (16 November 2018) *Business Law Blog*.

[99] Google v CNIL C-507/17 [2019] ECLI:EU:C:2019:15 (Advocate General, 10 January 2019) para 78.

[100] Google v CNIL C-507/17 [2019] EU:C:2019:772 (CJEU, 24 September 2019) para 73, but see also para 69.

[101] Contrast to arguments about the failings of territoriality made e.g., in De Hert (n 14).

[102] The difference between the effects doctrine and the objective territoriality principle, if there is one, is that the former appears to have no requirement that the effects on the territory must be a 'constituent

wrong originated (subjective territoriality principle). In relation to the former, the Permanent Court of Justice only required that a constituent element of the offence must have occurred on the State's territory which is all too easily established and certainly does not require a substantial effect:

> it is certain that the courts of many countries, even of countries which have given their criminal legislation a strictly territorial character, interpret criminal law in the sense that offences, the authors of which at the moment of commission are in the territory of another State are nevertheless to be regarded as having been committed in the national territory*, if one of the constituent elements of the offence, and more especially its effects, haven taken place there*.[103]

The objective territoriality principle has made appearances in State law in different incarnations. For example, it underlies the concept of 'result' crime (versus 'conduct' crime) traditionally used by common law courts;[104] and also provided the basis of the US 'effects doctrine' in the antitrust context in the 1970s to 1990s.[105] The various instances show that the impact on the territory need not be physical (as in *Lotus*) and can include economic and other intangible impacts. In contemporary globalised society with a huge diffusion of the economic effects of a single activity, this entails potentially numerous overlapping and at times conflicting regulatory claims by various States in respect of a single wrongful activity e.g., a cartel. In response, the moderate approach that looks for a more substantial territorial effect has some precedent in some statements concerning international law. Most notably, the reasonable effects test is embedded in paragraph 403 of the US Restatement (Third) of Foreign Relations Law (1986), which states that 'a state may not exercise jurisdiction … with respect to a person or activity having connections with another state when the exercise of such jurisdiction is unreasonable'.[106] Whether such exercise is 'reasonable' is made dependant on factors, such as the extent to which the activity has a substantial, direct or foreseeable effect upon the territory, the character of the activity, the degree to which the desirability of regulation is generally accepted, the existence of justified expectations, the importance of regulating the activity, the consistency of the regulation with traditions of the international systems, the interest of other States in regulating the activity and the likelihood of conflicting regulation.[107] The US has also adopted a targeting approach in the civil context, through its adaptation of the 'minimum contacts' test laid down in *International Shoe Co v Washington* (1945),[108] which gives a court personal jurisdiction over an out-of-State defendant whenever she had sufficient contacts with the forum so much so that an action would not offend 'traditional notions of fair

---

element' of the crime, although this is invariably established or can be achieved by framing the offence appropriately.

[103] *Lotus* (n 21) 23 [emphasis added].

[104] *DPP v Stonehouse* [1978] AC 55; *R v Treacy* [1971] AC 557; *R v Markus* [1975] 1 All ER 958; *Brownlie v State Pollution Control Commission* (1992) 27 NsWLR 78; *R v Toubya* [1993] 1 VR 226; Discussed In Matthew Goode, 'The Tortured Tale of Criminal Jurisdiction' (1997) 21(2) *Melbourne University Law* 411, 437ff.

[105] Vaughan Lowe (ed), *Extraterritorial Jurisdiction* (Grotius Publications Ltd 1983).

[106] Section 403(1) of the US Restatement (Third) of Foreign Relations Law (1986).

[107] Ibid., Section 403(2).

[108] *International Shoe Co v Washington* 326 US 310 (1945), The test is not applicable to *in rem* jurisdiction which has thus been asserted in a far more expansive way: *US v $734,578.82 in US Currency* 286 F 3d 641.

play and substantial justice'. Subsequently, *Hanson v Denckla* (1958) framed the test as one of 'purposeful availment' whereby an out-of-State defendant is subject to the jurisdiction of the court if it *purposefully availed* itself of the privilege of conducting activities within the local State, thus invoking the benefits and protections of its laws.[109] Adapted to the internet, for example, in *Plixer International, Inc v Scrutinizer GmbH* (2018)[110] a US court assumed personal jurisdiction over Scrutinize, a German company, in a trademark infringement case on the basis of its global web-based services that had attracted a fair number of US customers. Equally in *UMG Recordings Inc v Kurbanov* (2020)[111] a Virginian court had jurisdiction over a Russian's music piracy websites given the hundreds of thousands of Virginian visitors to the sites and the personalised advertising displayed on them.

Nonetheless, regardless of their virtues, neither a reasonable effects doctrine nor a targeting test are mandated by customary international law, and States are not required to forego jurisdiction based on negligible local effects.[112] However, in the online context, the objective territoriality principle, if interpreted thinly, gives rise to innumerable (potential) concurrent claims and (actual) compounding obligations on online actors. It creates de-facto universal jurisdiction which, as a head of jurisdiction, has been limited to a dozen *universally* condemned crimes, such as piracy, war crimes or crimes against humanity, and is clearly not meant to extend to the numerous and varying legal standards on various topics applicable to online activity. This overregulation could largely be alleviated by a more moderate destination approach which only gives *targeted* States the right to regulate the activity and requires forbearance by States which are also affected by the site but only marginally so. Moreover, jurisdiction focused on those foreign actors that have a significant effect on the territory is the most realistic way to accommodate online transnationality within national law and order.

The (Exclusive) Origin Approach

An alternative to the destination approach to online jurisdiction is the origin approach whereby online activity is subject *only* to the laws of the State in which the provider is established or where the site is hosted.[113] The advantages of this approach are, first, that the regulatory burden on online actors is fairly light as they have to comply only with their home rule; and, second, it does not create the enforcement deficit of the destination approach, as the to-be-regulated actor is within the enforcement reach of the State. Nonetheless, but for rare exceptions, States have rejected the origin approach to online jurisdiction – albeit *not* by foregoing their rights to regu-

---

[109] *Hanson v Denckla* 357 US 235, 253 (1958).

[110] *Plixer International Inc v Scrutinizer GmbH* (2018) WL 4357137 (1st Cir, 13 September 2018). For earlier cases, see e.g., *People v World Interactive Gaming Corporation* 714 NYS 2d 844 (1999) and *Young v New Haven Advocate* 315 F3d 256 (2002).

[111] UMG Recordings Inc v Kurbanov 963 F3d 344 (4th Cir 2020).

[112] Even in the US, the application of the moderate test was confined in *Hartford Fire Insurance Co v California* 509 US 764 (1993) to situations of a 'true conflict' between domestic and foreign law, i.e., where the application of domestic law would entail the violation of the foreign country's law. This occurs very rarely. Most laws 'conflict' by imposing compounding duties on the subject.

[113] For alternative possibilities, see *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 where the editorial office was in New York and the server in New Jersey; see also para 41, where the court noted alternatives: the location where the material was initially composed or the place of incorporation of the provider; Australian Law Reform Commission, *Choice of Law* (Report No 58, 1992) 57.

late local online actors, but by still assuming regulatory competence over online activity that is *not* based within their territory, as seen above.[114] Their behaviour is consistent with customary international law which has long recognised that the territoriality principle gives concurrent regulatory rights to the origin State (subjective territoriality principle) and destination States (objective territory principle).

The reason for the general unacceptability of the *exclusive* origin approach is that it undermines the regulatory control of destination States over their territories: there is very little point in prohibiting a drug in the offline world, if it can be bought legitimately online from a foreign provider whose State of origin does not prohibit it and who is not subject to local rules. This would make the lowest common regulatory denominator the governing standard for every State. A rare example of the exclusive origin rule is provided in the EU context by Article 3(2) of the Electronic Commerce Directive,[115] which requires Members States *not* to regulate providers of information society services *established* in another Member State.[116] The acceptability of the rule here is based on three pre-requisites. First, it requires relatively harmonised legal standards so much so that the foreign rule does not significantly clash with local standards. Although the origin rule in the Electronic Commerce Directive is not limited to the harmonised standards established in other parts of the Directive, it works against the background of substantial long-term steps taken towards harmonisation or approximation within the European internal market.[117] Second, the exclusive origin rule in the Directive is not simply a rule forbidding destination States to regulate providers from other Member States, but imposes a duty on the origin State to regulate their local providers.[118] This ensures that there is no regulatory vacuum. Third, the rule is based upon reciprocity, rather than being acceptable unilaterally: to the extent that States gain economic advantages by virtue of their companies being able to access foreign markets without the hurdles presented by different regulatory requirements, they also have to accept the opening of their market to foreign providers. The Directive's regime (along with the wider single market framework) creates that reciprocity amongst the Member States. For these reasons, an exclusive origin rule would not be acceptable to States internationally, barring the unlikely scenario that States entered into an inter-

---

[114] For example, *R v Perrin* [2002] EWCA Crim 747.

[115] Electronic Commerce Directive 00/31/EC.

[116] Art 2(c) of the Electronic Commerce Directive, 00/31/EC: 'a service provider … pursues an economic activity using a fixed establishment for an infinite period. The presence and use of the technical means and technologies required … do not, in themselves, constitute an establishment of the provider'. Julia Hörnle, 'Country of Origin Regulation in Cross-Border Media: One Step Beyond the Freedom to Provide Services?' (2005) 54 *International and Comparative Law Quarterly* 89, 113; and *Commission v UK* Case C222/94 [1996] ECR I-4025, concerning Art 2(1) of the Television Without Frontiers Directive 89/552/EC (later revised by 97/36/EC).

[117] Art 2(h) of the Electronic Commerce Directive. An earlier Directive that adopted the approach is, for example, Television without Frontiers Directive 89/552/EEC (revised by 97/36/EC), see Art 2a(1).

[118] Art 3(1):

> Each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field.

The destination State can first of all request the origin State to fulfil its duty and then take measures to restrict incoming services, after notifying the Commission and the origin State of its intention under Art 3(40(b) of the Directive; it can also initiate infringement proceedings under Art 226 or Art 227 of the EC Treaty.

national convention that, first of all, harmonised the legal standards to which it, then, applied the origin rule and combining a duty to regulate local providers with forbearance vis-à-vis foreign ones. Yet, as shown above, the jurisdictional wranglings are principally caused by the significant differences in the legal standards (and underlying values and economic interests) and thus the acceptability of the origin approach presupposes the very solution to the crux of the jurisdictional problem.

Even in the EU, the exclusive origin rule and its boundaries in Article 3(2) have been contested. There has been some debate on what amounts, in the online era, to an 'establishment' which provides the territorial touchstone in numerous European legislative instruments.[119] Furthermore, the substantive boundaries of the forbearance by destination States have come under scrutiny. In *Arzneimittelwerbung im Internet* (2006)[120] a German court held that a Dutch site advertising and selling drugs to Germans was subject to German licensing requirements even though the drugs were legal in the Netherlands, as the Directive was not applicable to national legal requirements concerning the physical delivery of goods[121] that were designed for the protection of public health.[122] This signals the importance of the topic of health and safety to national law spaces, but also the rather murky boundary between online and offline conduct.

4. ENFORCEMENT JURISDICTION ON THE INTERNET

The territorial restrictiveness of enforcement jurisdiction (as per *Lotus* 'the first and foremost restriction imposed by international law upon a State is that … it may not exercise its power in any form in the territory of another State'[123]) has made itself felt in two arenas of online transnationality – with opposite directionality. On the one hand, States have had to look for internal routes to enforce their legal standards vis-à-vis external online actors and activities. On the other hand, States have looked to external data to aid their internal law enforcement efforts. Thus, in the first instance, jurisdiction is implicated in the protection of national law space from being undermined by external sources, whilst in the second instance external resources may help to strengthen domestic law and order. In spite of the opposite directionality, in both instances States have heavily leaned on global platforms and other local intermediaries as law enforcement vehicles.

First, the blocking of online material or, more granularly, making some online material less easily accessible and thereby discouraging whatever is considered 'harmful' commu-

---

[119] Weltimmo sro v Nemzeti Adatvedelmi es Informacioszabadsag Hatsosag C-230/14 [2015] EUECJ, para 31, defining 'establishment' as any 'real and effective activity - even a minimal one - exercised through stable arrangements'; *VKI v Amazon* C-191/15 [2016] ECLI:EU:C:2016:612, para 76, a website's accessibility in a Member States does not constitute an establishment.

[120] *Arzneimittelwerbung im Internet* BGH (30 March 2006, I ZR 24/03). See also *Deutscher Apothekerverband eV v 0800 Doc Morris NV* C-322/01 [2003] ECR I-14887.

[121] Recital 21 and Art 2(h)(ii) of the Directive.

[122] Art 3(4)(a)(i) of the Directive. See also Art 87(1) of the Community Code for Medicinal Products for Human Use Directive 2001/83/EC (prohibition on the marketing of drugs for which there is no authorisation in accordance with Community law). Note too, that Art 13(7) of the WHO Framework Convention on Tobacco Control (Geneva, 2003) allows States to ban cross-border tobacco advertising (incl. advertising via the Internet).

[123] *Lotus* (n 21) 18.

nications (e.g., terrorist, political or hatred enticing) or conduct (e.g., gambling or piracy or anticompetitive trading) has come in a wide range of forms and attached to a wide range of online intermediaries. These fall along a spectrum of relative restrictiveness. One end of the spectrum is occupied by authoritarian regimes that block entire domains through backbone providers or Internet Access Providers. China is the most well-known example, but the practice is widespread. Although the legitimacy of such blocking only infrequently makes it before a non-national court, in *Yildirim v Turkey* (2013)[124] the European Court of Human Rights (ECtHR) had the opportunity to assess the court-ordered blocking of Google Sites through Turkish ISPs on the basis that a third-party site violated Turkish law on the protection of Ataturk's memory. The ECtHR held that Yildrim's freedom of expression had been violated; his site which was unrelated to the offending site but had become inaccessible due to the general block, formed part of the undue collateral damage of the blocking order.[125] Turkey had insisted that blocking access to Google Sites was the only technical means of blocking the one offending foreign site, but there was no evidence that Google had been put on notice of the material.[126] This practice of domain blocking (and implicit extensive censorship) is only one step removed from the practice, prevalent in many liberal democracies, of requiring local ISPs – via judicial orders – to block domains with a high frequency of piracy or trademark infringement, as affirmed in the UK Supreme Court judgment in *Cartier International AG v BT plc* (2018),[127] or – via executive requests[128] – to block terrorist sites. The difference to the authoritarian regimes lies primarily in the nature of the unacceptable content, and secondarily in the relative generalist importance of the blocked sites. Yet, in principle these orders are attractive to States in delivering a quick fix whenever they are not 'in a position to reach the perpetrators for prosecution or if their request for removal or take down of such content is rejected or ignored by foreign law enforcement authorities or hosting and content providers'.[129]

At the other end of the spectrum are the cases and legislative instances discussed above where platforms are asked to remove, or make inaccessible, specific third-party content as opposed to removing entire domains through Internet Access Providers. The early *Yahoo* judgment made Yahoo a border guard in respect of third-party content illegal in France by imposing a duty on Yahoo to block such content from being accessible on French territory. Similarly, *Google Spain* and *Google CNIL* require Google, and like providers, to re-enact – on a notice and takedown basis by users – EU territoriality in respect of data protection on its European domains, and residually on its non-European domains when accessed from EU terri-

---

[124] *Case of Yildirim v Turkey* No 3111/10 ECtHR (18 March 2013).

[125] Ibid., para 66.

[126] One question here is whether an expectation of self-censorship based on national legal requirements as was the case prior to the internet vis-à-vis communication bottlenecks, such as TV, radio and the press, is still legitimate vis-à-vis online intermediaries.

[127] *Cartier International AG & Ors v British Telecommunications plc & Anor* [2018] UKSC 28; see also *Twentieth Century Fox Film Corp & Ors v British Telecommunications plc* [2011] EWHC 1981. For a wider overview see Yaman Akdeniz, *Freedom of Expression on the Internet* (15 December 2011 OSCE).

[128] For example, for the UK, see s.3 of Terrorism Act 2006, and the Counter-Terrorism Referral Unit, critiqued in in Hörnle (n 1) 41ff, and in Brian Chang, 'From Internet Referral Units to International Agreements: Censorship of the Internet by the UK and the EU' (2018) 49 *Columbia Human Rights Law Review* 116.

[129] Akdeniz (n 127) 6.

tory.[130] Most explicitly, the *German Network Enforcement Law* (2017) makes large platforms law enforcers in respect of the content shared on them in line with German law on hate speech, misinformation etc., and this applies equally to content uploaded within and outside Germany. Although platforms have sought to resist these costly takedown obligations, amongst others on the ground of the excessive discretion implicit in implementing the obligations, there is in fact a long-standing tradition of using corporate bottlenecks as gatekeepers, or quasi-law enforcement vehicles, most notably media companies, payment providers or supermarkets, albeit traditionally of more national standing. The willingness of the global platforms to oblige stems from their desire to gain or retain market access and not being seen as a rogue player – regardless of whether there is any real enforcement threat by public authority.[131]

Whilst these two ends of the spectrum differ in the expansiveness of the blocked or removed content and in the expected input by corporate gatekeepers, they are also counterparts that work in unison. The resource intensive task of removing specific unacceptable content is transferred to platforms and other intermediaries through the notice-and-takedown process against a State's ultimate power to block platforms that fail to do so. Meanwhile the 'privatised' removal process started by users and completed by platforms weakens the sting of accusations of State censorship that attaches to judicial or executive blocking orders,[132] and thereby allows for regulatory gains without the attendant accountabilities. Yet, platform censorship also carries the risk of significant collateral speech damage.[133] The inevitable side effect of blocking orders *and* notice-and-takedown processes is the territorial fragmentation of the internet, as driven by the objective of protecting national political, cultural and economic stakes.[134]

Second, overt jurisdictional wrangling has in recent years concentrated in the arena of criminal investigation where police and prosecutors have sought access to data held on overseas servers.[135] Against the revelations by Edward Snowden and, in particular, the integral involvement of key platforms in the NSA's PRISM programme,[136] platforms have sought to resist information requests by public authority more strongly. Most publicly, such resistance came to a head in *Microsoft Corp v United States* (2016)[137] where Microsoft sought to resist

---

[130] For content beyond data protection compliance, see European Commission, 'EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online' (3 December 2015, IP/15/6243).

[131] Matt Sheehan, 'How Google took on China – and lost' (19 December 2018, *MIT Technology Review);* Hannah Jane Parkinson, 'Uber offices raided in Paris by French police in "car-pooling" controversy', *The Guardian* (18 March 2015) https://www.theguardian.com/technology/2015/mar/18/uber-offices-raided-in-paris.

[132] Chang (n 128).

[133] See, e.g., French Constitutional Court, above n 52. The German Network Enforcement Law (2017) attempts to provide some State oversight of such private removal activity through reporting and publishing requirements in respects of complaints and removed content, and platforms also have to respond to information by administrative authorities.

[134] 'Data Protection: Angela Merkel proposes Europe network', *BBC News* (15 February 2014) http://www.bbc.co.uk/news/world-europe-26210053.

[135] For the whole spectrum of such transnational law enforcement activities, see Ian Walden, 'Accessing Data in the Cloud: the Long Arm of the Law Enforcement Agent' (2011) Queen Mary School of Law Legal Studies Research Paper No. 74/2011; Hörnle (n 1) 54 *ff*.

[136] See n 14.

[137] *Microsoft Corp v United States* 829 F3d 197 (2d Cir 2016); *In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp* 15 F Supp 3d 466 (SDNY 2014); see https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2

a search and seizure warrant (issued in 2013) concerning the content of all emails belonging to a suspect (the nationality of whom was not known[138]) in a drug-trafficking investigation, and related account information – on the basis that the email was stored on its Irish server and thus outside the legitimate application of search warrants. For the judge granting the order and the first court of appeal, a warrant requiring access to data (under the Stored Communications Act 1986[139]) was not comparable to normal (physical) search and seizure warrants for transnational purposes, as US law enforcement did not have to set a foot onto Ireland; Microsoft itself could comply with the order from its US headquarters. The information stored in Ireland could be had in the US at a push of a button on US territory; and so, it was argued, there was no question of extraterritoriality. Indeed, there is no denying that data within network society *is* different from physical documents; the extreme ease of its transferability and the happenstance of its 'location' makes arguments based on the significance of that location contrived and artificial. For this very reason, the location of servers has never been significant in the context of legislative or adjudicative jurisdiction over online activity. Meanwhile, it was *not* artificial to focus on the location of Microsoft in the US and its consequential allegiance to the US law space.[140]

Ireland submitted an Amicus Brief in Microsoft's appeal to the US Court of Appeals for the Second Circuit in New York, arguing that such data access and transfer would violate its territorial sovereignty, particularly as the alternative avenue of a formal request under a Mutual Legal Assistance Treaty (MLAT) had not been pursued.[141] This argument seems disingenuous, partly, because information requests of this or similar kind through local private actors are not particularly exceptional,[142] and have also been used in Ireland,[143] and, partly, because MLAT requests have proven exceptionally cumbersome in operation.[144] Whilst the Second Circuit Court reversed the decision by ostensibly taking the location of the requested data seriously ('the data lies within the jurisdiction of a foreign sovereign'[145]), it implicitly opened the door to more expansive legislative developments by treating the investigatory process (and the search warrants) as part of legislative/adjudicative jurisdiction to which the presumption against extraterritoriality could apply and in fact applied, and could also be set aside, where desired

---

-0/; discussed in De Hert (n 14); Editor, 'Microsoft Corp. v. United States – Second Circuit Holds that the Government Cannot Compel an Internet Service provider to Produce Information Stored Overseas' (2016) 130 *Harvard Law Review* 769.

138 *Microsoft Corp v United States* 829 F3d 197, 230 (2d Cir 2016).

139 18 U.S.C. §§2701-2712.

140 Note, e.g., that antisuit injunctions, although used in the civil context, could be, and have been, seen as an interferences with sovereignty of the State whose court processes are to be stopped, but are routinely justified on the basis of being directed solely to the person subject to the jurisdiction of the court making the order. So the foreign interference is disguised behind the relational link with the person to whom the order is addressed.

141 See Brief submitted on appeal to the Supreme Court (later abandoned): *Brief for Ireland as Amicus Curiae in Support of Neither Party* (No 12-2, 9 November 2017) https://www.supremecourt.gov/DocketPDF/17/17-2/23732/20171213152516784_17-2%20ac%20Ireland%20supporting%20neither%20party.pdf.

142 See discussion of the Belgium cases in Hörnle (n 1) 58ff.

143 *Walsh v National Irish Bank* [2013] IESC 4, where the court left open the possibility of ordering the disclosure of information from a foreign branch, even where compliance with such order would be in breach of foreign law, as acknowledged in the Ireland's Amicus Curiae; (n 141) 5.

144 See, e.g., discussion in Andrew Keane Woods, 'Mutual Legal Assistance in the Digital Age' in David Gray, Stephen E Henderson, *The Cambridge Handbook of Surveillance Law* (CUP 2017) 659.

145 *Microsoft Corp v United States* 829 F3d 197, 220 (2d Cir 2016).

by the legislature.[146] In contrast, for enforcement jurisdiction, there is no presumption against extraterritoriality as *all* public acts on the territory of another State are illegitimate interventions, and cannot be legislated away by the interfering State. By implication, the Second Circuit Court did not, after all, assume that accessing and transferring of data from Ireland through a US intermediary (which the court rightly considered a governmental agent at the point of the warrant[147]) involved any real interference with the territory of Ireland, and could thus be legalised through appropriate legislation in the US. Thus for the Court, governmental requests relating to foreign data lay after all outside the strict territorial limits of enforcement jurisdiction applicable to physical interferences.

The Court paved the way for the *Clarifying Lawful Use of Data Act* (2018), known as the *Cloud Act*,[148] through which Congress expressly rebutted the presumption against extraterritoriality by obliging providers of electronic communication services to 'disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States'. Although the Act presents a unilateral assertion of jurisdiction over all data controlled by local platforms regardless of its location, it also makes a half-hearted gesture to the reciprocal and cooperative spirit of the MLATs. It allows for a search warrant to be challenged (and quashed) on the grounds of comity where the data relates to a non-US person (absence of domicile and citizenship) *and* where there is a conflict with the laws of a State which had entered into an 'executive agreement' to give access to meta and content data of its service providers.[149] In light of this expansive legislative stance, set against the US's overall data dominance, it seems not unreasonable for other States to co-opt the very same platforms in *their* investigation of *their* local crimes, whenever these platforms have a 'commercial presence' within their territories, irrespective of any physical establishment. This occurred in the two cases of *Belgium Yahoo* (2015) and *Belgium Skype* (2016),[150] and should not be considered harsh. Just because Yahoo and Skype do not have a physical presence in Belgium does not absolve them of legal compliance. This would, after all, be the logical consequence of characterising requests for data as instances of legislative/adjudicative jurisdiction, rather than enforcement processes, and then also be consistent with that jurisprudence. Alternatively and more appropriately, these requests for evidence can be seen as enforcement activities that, due to the quasi-intangible nature of data, require no physical entry on to another State's territory.

---

[146] Albeit in the case of the Stored Communications Act the presumption, whilst triggered, had not been set aside by the legislature.

[147] *Microsoft Corp v United States* 829 F3d 197, 214 (2d Cir 2016) ('When the government compels a private party to assist it in conducting a search or seizure, the private party becomes an agent of the government, and the Fourth Amendment's warrant clause applies in full force to the private party's actions').

[148] 18 USC §2713, see Hörnle (n 1) 57 *f*. For the equivalent EU legislative proposal on e-evidence in criminal matters: Proposal for a Regulation of the European parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final (Strasbourg, 17 April 2018).

[149] 18 USC § 2703 (h) (2).

[150] *Belgium Yahoo* (Nr. P.13.2082.N, Belgian Supreme Court, 1 December 2015); *Belgium Skype* (Belgian Court Appeal, 15 November 2017) https://www.reuters.com/news/technology/article/us-skype-belgium-court/skype-loses-belgian-court-appeal-after-fails-to-comply-with-call-data-order-idUSKBN1DF1MA; discussed in Hörnle (n 1) 59 *f*.

5. CONCLUSION

Jurisdiction continues to be a live issue within the arena of network regulation and to evolve in line with wider regulatory trends. Its areas of controversy have shifted from the question of when a State may or may not exercise regulatory competence across a wide spectrum of concerns over global online activity, to more pragmatic questions such as when and how global platforms and their wealth of (personal) data may be used to maintain and even enhance territorial sovereignty, as a matter of internal order and external competitiveness.

It remains true that the objective territoriality principle under customary international law is frequently stretched to its maximum in order to extend national law to online activity, which is in itself an entirely legitimate endeavour. From an internal perspective, States are legitimately concerned about foreign online activities undermining local law and order, no matter how marginal that external interference may be. Yet, from a global perspective, the unmoderated application of national law to the transnational internet cannot but lead to the territorial fragmentation of the internet into national cyberspaces with attendant costs for freedom of expression as well as for economic, political, social and cultural exchange. Arguably, the transnational internet is suffering the tragedy of the commons or a death by a thousand cuts: each time a State asserts its right to apply its peculiar regulatory version of the 'good life' to the online world and each time this assertion is enforced via border blocking or notice and takedown removals, transnationality is slightly impeded. The moderate approach to territorial jurisdiction that looks to *substantial* effects as a trigger for State competence and legal obligations of online actors presents a more realistic regulatory burden on both public authority and online actors, whilst creating porous rather than solid territorial online borders, and placing trust in users to be able to deal with foreign legal Otherness.

Contrary to the conclusion reached by this chapter in the first edition of this Handbook, this chapter posits that global network society does not significantly weaken the authority of the territorial State, and even promises (or threatens, depending on one's perspective) to enhance it, *as long as* the State acts in partnership with dominant global platforms as gatekeepers and data collectors. When these platforms share the unprecedented wealth of personal data, and their concomitant intimate knowledge of online users – including their location, movements, preferences, activities, and psychological states – with public authority, this creates entirely new opportunities for expanding and deepening control over citizens and their activities. By the same token, the intangible and slippery nature of data is not counterproductive to territorial-based jurisdiction *if* its controllers can be co-opted into sharing it with the State, regardless of *where* it may slumber. Territoriality, although tied to a physical space, is ultimately a socio-legal construction denoting dominion or authority, and that dominion depends on access to data – consolidated into information and then transformed into knowledge – as its lifeblood.

5. The international law of cyber intervention

Ido Kilovaty

1. INTRODUCTION

Non-intervention is a bedrock principle of modern international law.[1] Non-intervention, deriving its rationale primarily from territorial sovereignty,[2] sovereign equality,[3] and political independence[4] prohibits States from coercively interfering in the domestic or foreign affairs of other States.[5] Non-intervention's centrality to the international legal system was illustrated by the then-Permanent Court of International Justice, observing that: 'the first and foremost restriction imposed by international law upon a State … [is that] it may not exercise its power in any form in the territory of another State'.[6] The importance of the principle of non-intervention has also been confirmed by the International Court of Justice.[7]

But what does it mean for a State to *intervene* and thus violate the principle of non-intervention? The International Court of Justice (ICJ) in the *Nicaragua case* iterated that non-intervention denotes 'the right of every sovereign State to conduct its affairs without outside interference'[8] and that prohibited intervention is 'one bearing on matters in which each

---

[1] See *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America),* 27 June 1986, ICJ Reports 1986, para 202 ('the Court considers that it is part and parcel of customary international law') (hereinafter *Nicaragua*).

[2] Michael N Schmitt and Sean Watts, 'Beyond state-centrism: international law and non-state actors in cyberspace' (2016) 21 *J. Conf. and Sec. L.* 595, 600 ('The prohibition of intervention by a state into the internal or external affairs of other states derives directly from the principle of sovereignty'). On sovereignty in cyberspace see Tsagourias (Ch 1 of this Handbook).

[3] E.g., Art 2(1) of the UN Charter ('The Organization is based on the principle of the sovereign equality of all its Members') and Art 2(7):

> Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII.

[4] Robert Jennings and Arthur Watts, *Oppenheim's International Law. Intervention*, 1 (OUP 2008) 430–49.

[5] G.A. Res. 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (24 October 1970) (hereinafter Friendly Relations Declaration):

> No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of another State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.

[6] *S.S. Lotus* (France v. Turkey) [1927] PCIJ (Ser. A) No. 10, 18.

[7] *Corfu Channel Case* (UK v. Albania), Judgment [1949] ICJ Rep 4, 35 (hereinafter *Corfu Channel*); *Nicaragua* (n 1) paras 202, 205, 25; *Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda)*, Judgment [2005] ICJ Rep 168, paras 161–165 (hereinafter *Armed Activities*); Friendly Relations Declaration (n 5) para 3.

[8] *Nicaragua* (n 1) para 205.

State is permitted, by the principle of State sovereignty, to decide freely'.[9] In other words, non-intervention is a specified prohibition stemming from the logic of sovereignty in that States are at liberty to conduct their internal and external affairs free of foreign intervention.[10]

However, the emergence of State-sponsored cyber operations that seek to interfere in the domestic and foreign affairs of another State change through the use of cyber-attacks,[11] digital election interference,[12] and deep fakes,[13] and paired with the growing role of social media platforms has seriously challenged the efficacy, relevancy, and clarity of the principle on non-intervention. Primarily, the two constitutive elements of non-intervention – coercion into the *domaine réservé* – are becoming increasingly difficult to apply in the context of cyber operations.

Perhaps this irrelevancy is best exemplified by the activities constituting the Russian interference in the 2016 US election. Some activities in which Russia was involved, such as hacking voter rolls, may be in clear violation of the principle. However, other acts of interference which are just as detrimental to the political process pose more of a challenge to the principle. Are disinformation campaigns on social media in violation of the principle? Is it wrongful to use political bots to sway public opinion on the eve of a presidential election? What about doxing of a political organization such as the Democratic National Committee?[14] Are deep fakes 'coercive' and therefore unlawful?

The ambiguity with regard to non-intervention exists notwithstanding the fact that the prohibition on intervention is sprinkled throughout international law – in both treaties and custom.[15] It has gained wide acceptance in the international community and has been reaffirmed multiple times in different international contexts.[16] Nonetheless, States have done little to clarify the contents of the norm,[17] setting non-intervention on a path of becoming irrelevant in the coming decades, unless States do more to adapt non-intervention to emerging forms of interference enabled by cyberspace and new technologies.

Non-intervention's two constitutive elements – *domaine réservé* and coercion – are both challenged by the emergence of cyberspace as a tool and domain of interference. Cyberspace

---

[9] Ibid.

[10] Nicholas Tsagourias, 'Electoral cyber interference, self-determination, and the principle of non-intervention in cyberspace' in Dennis Broeders and Bibi Van Den Berg (eds), *Governing Cyberspace Behavior, Power and Diplomacy* (Rowman and Littlefield 2020).

[11] See e.g., Oona Hathaway *et al*., 'The law of cyber-attack' (2012) 100 *California Law Review* 817.

[12] See e.g., Nicholas Tsagourias, 'Electoral cyber interference, self-determination and the principle of non-intervention' (6 August 2019) EJIL: *Talk!*, https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/.

[13] See e.g., Robert Chesney and Danielle Citron, 'Deepfakes and the new disinformation war' (January 2019) *Foreign Affairs*.

[14] Michael N Schmitt, 'Grey zones in the international law of cyberspace' (2017) 42 *Yale Journal of International Law* 1, 2 ('It is unclear whether facilitating the release of actual emails—as distinct from, for example, using cyber means to alter election returns—amounts to coercion as a matter of law').

[15] *Corfu Channel* (n 7) 35; *Nicaragua* (n 1) paras 202, 205, 251; *Armed Activities* (n 7) paras 161–165; Friendly Relations Declaration (n 5) para 3.

[16] Ibid.

[17] Sean Watts, 'International law and proposed U.S. response to the D.N.C hack' (14 October 2016) *Just Security*, https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/ ('Although the prohibition of intervention is longstanding, States have not done much to clarify precisely where this threshold of coercion lies').

as a domain of interference, emerging technologies, and new platforms of communications are currently challenging these two elements.

This chapter is focused on the international law of cyber intervention. It reflects on emerging interference technologies, cyberspace, and non-intervention. It then argues that the foundations of non-intervention, as understood pre-cyberspace, are untenable given these global cyberspace and technological trends. The purpose of this chapter is to look at the elements of non-intervention and the way in which they are challenged in light of this technological context. In addition, this chapter offers some directions for non-intervention in the cyber era: expanding coercion, looking to human rights, and considering the growing role of manipulation, disinformation, and disruption.

The chapter constitutes of two parts. First, this chapter will introduce the norm of non-intervention. Second, this chapter will make some observations with respect to non-intervention in cyberspace. These observations are both descriptive (what current gaps and ambiguities there are) and normative (what can or needs to be done to alleviate some of these gaps and ambiguities).

2. NON-INTERVENTION

The modern conception of the principle of non-intervention is understood to contain two constitutive elements. These two elements transform an act of mere interference,[18] which is not illegal under international law, to an act of intervention, which is unlawful under international law.[19] Both elements are required in order to hold a State accountable for a violation of non-intervention.

An act of unlawful intervention must, first, be directed at certain sovereign prerogatives, namely the *domaine réservé*,[20] and; second, it must be *coercive*.[21] This section considers the content of these two elements in the following two sub-sections.

2.1 *Domaine Réservé*

In order to be wrongful under international law, an act of interference must target a specific subset of protected State prerogatives, referred to as *domaine réservé*. These prerogatives derive their legitimacy from the State's sovereignty and political independence, and any

---

[18] By 'interference' I mean 'activities that disturb the territorial State's ability to perform the functions as it wishes'. Though, interference by itself is currently not illegal under international law, unless it is coercive and targets the *domaine réservé*. See Michael N Schmitt, '"Virtual" disenfranchisement: Cyber election meddling in the grey zones of international law' (2018) 19 *Chicago Journal of International Law* 30, 45.

[19] Jennings and Watts (n 4) 432 ('the interference must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question. Interference pure and simple is not intervention').

[20] *Nicaragua* (n 1) 205. Also see Jens David Ohlin, 'Did Russian cyber interference in the 2016 election violate international law?' (2017) 95 *Texas Law Review* 1579, 1587 (a State's *domaine réservé* refers to 'its exclusive power to regulate its internal affairs without outside interference').

[21] *Nicaragua* (n 1) para 205 (June 27) ('Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, […] defines, and indeed forms the very essence of, prohibited intervention').

outside coercive interference with them is impermissible. Conceptually, the logic behind *domaine réservé* appears intuitive. Yet, the exact contents of *domaine réservé* can sometimes be unclear.[22]

The International Court of Justice (ICJ) in the *Nicaragua* decision, has provided some guidance on the contours of *domaine réservé*. The ICJ explained:

> a prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.[23]

In similar vein, Michael Schmitt, attempted to draw the line between matters under the sole discretion of the State and those that are not.[24] Schmitt provides that 'elections fall within the *domaine réservé*' while 'commercial activities typically do not'.[25] Intuitively, if a State engaged in an act of interference 'intended to afford business advantages to its national companies' it would not run afoul of the principle on non-intervention. Yet, Schmitt's characterization is missing an important context, where different regimes are likely to have different sovereign prerogatives, and thus the concept of *domaine réservé* would differ depending on the specific regime.

While these two extremes drawn by Schmitt are uncontroversial, Schmitt also acknowledges that there may be a grey zone in the context of online communications.[26] States typically regulate online communications to a certain degree; yet, this is not within the sole discretion of the regulating State.

The example of communications as a realm owned and maintained by private entities while also regulated (to different degrees) by States may complicate our assessment of whether an act of interference is directed at sovereign prerogatives that are part of the *domaine réservé é* or not. Therefore, the question in that case would be: does foreign interference with online communications constitute an act against the *domaine réservé* of the victim State? The answer, to many, is in the negative. But what about the *should* question? *Should* it be unlawful for States to interfere with other States' online communication or political discourse on social media platforms taking place abroad? International law has not been able to address this timely question, particularly given the growing role of private speech platforms, namely social media, which have become the new public squares enabling not only communications and speech locally, but also across the globe. Is the notion of *domaine réservé* still relevant in a world where social media platforms have transformed online communications and political campaigning?

---

[22] Ohlin (n 20) 1588; Schmitt (n 18) 45:
The inherently governmental function concept lacks granularity, although some cases are clear. On the one hand, purely commercial activities, even if engaged in by State-owned enterprises, do not qualify, for they obviously are not within the exclusive purview of a State. On the other hand, law enforcement and defense of the State from external attack are inherently governmental in character… Between these extremes lies a great deal of uncertainty.

[23] *Nicaragua* (n 1) para 205.

[24] Schmitt (n 14) 7.

[25] Ibid.

[26] Ibid.

2.2 Coercion

Coercion is a central element of non-intervention. In *Nicaragua,* the ICJ exemplified the importance and centrality of coercion to the norm of non-intervention, where it held that 'intervention is wrongful when it uses methods of coercion'[27] and that coercion is 'the very essence'[28] of intervention. As such, an act of coercion in relation to 'matters of inherently sovereign nature' constitutes unlawful intervention.[29]

In similar spirit, in the *Corfu Channel* case, the ICJ rejected the argument that there is a 'right of intervention' recognized by international law, by noting that it views 'the alleged right of intervention as the manifestation of a policy of force, such as has, in the past, given rise to the most serious abuses'.[30]

In addition, the 1970 Declaration on Friendly Relations provides that:

> No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind.[31]

Non-intervention and the coercion requirement carry to the cyberspace context as well. The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* provides that 'States may not intervene, including by cyber means, in the internal or external affairs of another State'[32] and subsequently clarifies that in order to be wrongful under international law, such intervention 'must be coercive in nature'.[33]

According to this widely accepted view, there can be no unlawful intervention without coercion. Any act of interference falling below the threshold of coercion is not unlawful under international law. For example, Jamnejad and Wood suggest that 'Only acts of a certain magnitude are likely to qualify as coercive.'[34] Though, such magnitude threshold is not fully established under international law.

In similar vein, Oppenheim conceptualized coercion in terms of 'control'. According to this view, whenever a State is deprived of control over a matter by an external force, an act of coercion has occurred.[35] Oppenheim, however, provides some useful guidance on coercion, by asserting that to qualify as prohibited intervention, 'interference must be *forcible or dictatorial, or otherwise coercive; in effect depriving the State intervened against of control over the matter in question*'.[36] In other words, an act of coercion exists when the victim State is *forced*

---

[27] *Nicaragua* (n 1) para 205.

[28] Ibid.

[29] Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, Chatham House (2019) 27, https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks.

[30] *Corfu Channel* (n 7) 35.

[31] UN Doc. A/RES/2625 (XXV).

[32] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) Rule 66 (hereinafter Tallinn Manual 2.0).

[33] Ibid.

[34] Maziar Jamnejad and Michael Wood, 'The principle of non-intervention' (2009) 22 *Leiden Journal of International Law* 345, 348.

[35] See Tsagourias (n 10) 52.

[36] Jennings and Watts (n 4) 430–49.

to do something by an external State actor, or when it is faced with an ultimatum – do X (or refrain from doing X), or else.[37]

Schmitt, similarly, defines an act of coercion as an action 'intended to cause the State to do something, such as take a decision that it would otherwise not take, or not to engage in an activity in which it would otherwise engage'.[38]

Coercion, therefore, is an action that deprives the State of its sovereign will. It is an action that seeks 'to force a policy change in the target state'.[39] A State loses its independence when its sovereignty is forcefully delegated by an external State actor. But sovereign will and independence may still be undermined even if something other than the *domaine réservé* is targeted, or when interference is not designed to be *coercive.* Consider for example a foreign State government who is engaged in microtargeting users on social media with disinformation, leading to a certain outcome in the victim State. Non-intervention is unlikely to be relevant in this context, unless it deprives the victim State of control over a matter in question, with the matter constituting part of its protected *domaine reserve*.

These conceptions of coercion raise some complicated questions in the cyber era. For example, what is coercion's requisite threshold of magnitude? Does deprivation of control need to be total, or can it be partial? What if an initial act of influence or interference leads to a chain of events that in the result deprives the victim State of control over a certain matter? The relevant instruments on non-intervention do not provide a clear answer to these questions, which may signify that non-intervention suffers from a serious gap in the cyber era.[40] After all, if there is no intervention without coercion, and there is no robust theory on what coercion is, then the legitimacy and efficacy of the principle dissipates.

3. NON-INTERVENTION AND CYBERSPACE

The gap in international law with respect to non-intervention is partially due to the rapid evolution of technology vis-à-vis the international legal systems.[41] In other words, the principle of non-intervention 'fail[s] to keep pace with technological advancements that render territorial limits irrelevant'.[42] It is not only technology that has made significant advancements in recent decades, but also the non-State actors involved in this space, who are increasingly powerful. The implication is that States do not need coercive tools to unduly and substantially influence internal or external affairs of another State,[43] and they do not need to target their operations

---

[37] Ido Kilovaty, 'The elephant in the room: Coercion' (2019) 113 *American Journal of International Law Unbound* 87, 89; Moynihan (n 29) 28.

[38] Schmitt (n 18) 51.

[39] Jamnejad and Wood (n 34) 348.

[40] Ohlin (n 20) 1581 ('there is little in international law that outlines a complete theory of coercion'); Vaughan Lowe, *International Law* (OUP 2007) 104 (describing non-intervention as 'elusive').

[41] See generally Ryan Jenkins, 'Is Stuxnet physical? Does it matter? (2013) 12 *Journal of Military Ethics* 68, 69.

[42] Simon Chesterman, 'Secret intelligence' (2009) Max *Planck Encyclopedia of Public International Law*, para 23, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e992?rskey=wEFJF5&result=1&prd=EPIL [https://perma.cc/R9LK-AMAT].

[43] See Duncan Hollis, 'Russia and the DNC hack: What future for a duty of non-intervention?' (25 July 2016) *Opinio Juris*, http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention/ ('looking at the DNC hack, there's little evidence that Russia is trying to

directly against State functions. On that point, Lori Damrosch argues that the current standard of coercion is 'unsatisfactory, because some subtle techniques of political influence may be as effective as cruder forms of domination'.[44] Nonetheless, international law's current challenge is to draw the line between lawful and unlawful influence, whether subtle or not.[45]

These shifting notions of what constitutes non-intervention are not in themselves unprecedented. During the nineteenth century, international law afforded States protection only for their territorial integrity. Not until the twentieth century did the scope of non-intervention expand to protect political independence.[46] Yet again, non-intervention is at a crossroads, where emerging interference technologies and cyberspace call for a reconsideration of non-intervention's scope.

3.1 *Domaine Réservé* is Difficult to Delineate in Cyberspace

The concept of *domaine réservé* assumes that protected State prerogatives, such as domestic and foreign affairs, can be neatly labelled and distinguished from activity, usually that which is not in the sole discretion of a State, that is not protected from foreign interference.

For once, the ever-blurring line between State and non-State is making the distinction between the protected and unprotected nearly impossible. For example, would the spread of disinformation on a private social media platform count as an intervention with the election system? Does targeting users with fake news on their elected officials count as intervention with the political system? Since private internet actors, such as Facebook and Twitter, fulfil no sovereign function, it seems antithetical to consider any activity taking place on these platforms as '*domaine réservé*'.

But it is not only the distinction between State and non-State that complicates the analysis, but rather the increasing power of non-State actors, such as social media platforms, political consulting firms, data analytics companies, and hacking groups. Given that non-intervention requires State action, and often a State target, these non-State groups need to be under a certain degree of control by a State actor in order for non-intervention to be relevant.[47] This is of course a question of attribution, but assuming that no State is involved, it highlights the shortcomings of the overreliance on the existing understanding of non-intervention as an interstate norm.

---

coerce any particular result. Indeed, it's not even clear that the goal of the hack was to support Trump's candidacy').

[44] Lori Damrosch, 'Politics across borders: Non-intervention and non-forcible influence over domestic affairs' (1998) 83 *American Journal of International Law* 5.

[45] Statement of Sir Ian Sinclair on behalf of the UK government (1966), Official Records of the General Assembly, 25th session, UN Doc A/AC.125/SR.114, Supplement No. 18 (A/8018) 155:

> it is inevitable and desirable that States will be concerned with and will seek to influence the actions and policies of other States, and that the objective of international law is not to prevent such activity but rather to ensure that it is compatible with the sovereign equality of States and self-determination of their peoples.

[46] Johannn-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law* (Intersentia 2014) 116.

[47] Schmitt (n 18) 48 (actions of non-State actors need to be attributable to a State 'through instructions [by a State] to, or [State] control over, non-State actors such as IT companies, hacker groups, or terrorist organizations'). Also see Art 8 of the Draft Articles on State Responsibility for Internationally Wrongful Acts 2001.

This creates a very appealing opportunity for States considering influence or interference operations. As exemplified by the Russian interference in 2016, States do not need to direct their operations at purely State targets or sovereign prerogatives to successfully interfere with a domestic political process. They can achieve the same goal by leveraging the reach and scale of social media platforms, microtargeting methods, and manipulation techniques. Indeed, the 2016 US election interference, as well as other election interferences throughout the world, consisted of cyber operations that 'expose, disgrace, or otherwise undermine a particular individual, campaign, or organisation in order to influence public opinion during an election cycle'.[48]

Indeed, Pavel Zolotarev, retired Russian general, strengthened this conclusion by saying that 'we had come to the conclusion, having analyzed the actions of Western countries in the post-Soviet space—first of all the United States—that manipulation in the information sphere is a very effective tool'.[49] In other words, to make a State pursue a policy that it otherwise would not,[50] States can design their operations to take advantage of the internet, its widespread reach, and the ability to manipulate its users.

On this point, Brian Egan similarly identified '[T]he very design of the Internet'[51] as an enabler of 'encroachment on other sovereign jurisdictions'.[52] According to Egan, some of the difficult questions presented with respect to international law and cyberspace 'ultimately will be resolved through the practice and *opinio juris* of States'.[53] Cyberspace is therefore exacerbating the ambiguity surrounding the norm of non-intervention.

This challenge is further exacerbated by technological innovation that would allow States to use even more sophisticated methods to interfere with a domestic process without targeting any *domaine réservé* targets. This phenomenon leads to a fragmentation, decentralization, and somewhat of a privatization of the *domaine réservé*. For example, while it is largely uncontested that coercive interference with the election infrastructure would constitute prohibited intervention, it would not necessarily be the case if coercive interference is aimed at social media platforms where voters debate and seek information on election-related matters.

Consider the following hypothetical involving deep-fake technology. Deep-fake technology represents a new threat to democracy globally.[54] Deep fakes are fabricated videos or audios, utilizing machine learning algorithms 'to insert faces and voices into video and audio recordings of actual people'[55] with the purpose of creating 'realistic impersonations… making it appear that someone said or did something'.[56] What if such deep-fake technology is deployed to spread disinformation about a candidate?

---

[48] Tsagourias (n 12).

[49] Evan Osnos, David Remnick and Joshua Yaffa, 'Trump, Putin, and the New Cold War', *The New Yorker* (24 February 2017).

[50] *See* Philip Kunig, 'Prohibition of intervention' (2008) *Max Planck Encyclopedia of Public International Law*, para 1 (intervention 'aims to impose certain conduct of consequences on a sovereign state').

[51] Brian J. Egan, Legal Adviser, US Dep't of State, *Remarks at Berkeley Law School on International Law and Stability in Cyberspace* (10 November 2016).

[52] Ibid.

[53] Ibid.

[54] See e.g., Bobby Chesney, Danielle Citron, 'Deep fakes: A looming challenge for privacy, democracy, and national security' (2019) 107 *California Law Review* 1743.

[55] Ibid., 4.

[56] Ibid., 4–5.

The introduction of deep-fake technology would challenge the basic tenets of non-intervention. Among the harms identified by Bobby Chesney and Danielle Citron in their article on deep-fake technology are distortion of democratic discourse, manipulation of elections, undermining diplomacy, and jeopardizing national security, and more.[57] On that point, Nicholas Tsagourias points out that deep fakes may constitute unlawful intervention if they are 'designed and executed in such a way as to manipulate the cognitive process where authority and will are formed and to take control over peoples' choices of government'.[58]

Tsagourias's view is crucial in that it shifts the focus from State authority and control to the people who collectively shape the decision-making of their respective governments. This approach is desirable if we are to respond to the challenging nature of technology and the digital information space, but further issues will need to be fleshed out in the years to come. For example, does non-intervention apply where an act of coercive interference is aimed at a private actor (e.g., a social media platform)? Does spreading disinformation count as 'coercion'? Are there any other human rights that could inform the appropriate scope of non-intervention (e.g., the right to privacy, freedom of speech, freedom to seek, receive, and impart information)?

3.2 Coercion is a Poor Fit for Cyber Operations

Interference becomes wrongful when it targets the *domaine réservé* using coercive methods. Coercion is the mischief that international law seeks to condemn, because it follows the logic that coercion is the sole method by which sovereign will can be subordinated.[59] If a State 'complies freely'[60] or 'the pressure is such that could reasonably be resisted'[61] then there is no subordination of sovereign will.[62] What follows is that acts that are not coercive, are by definition outside of the scope of non-intervention. The caveat is that there is a lot between volitional compliance and coercion. As ICJ Judge Rosalyn Higgins observed 'not all maximally invasive acts are unlawful, and not all minimally invasive acts are lawful'.[63]

Non-intervention is a norm that emerged in an era where coercion was almost exclusively the method of effective intervention. Coercion puts an ultimatum in front of the victim State: *do X (or refrain from doing X), or else*. There are very good reasons why coercion is wrongful under international law, but delimiting non-intervention only to acts that are coercive misses an important point, which is that interference in this day and age may use new technological methods that can be extremely harmful and detrimental to sovereignty, self-determination, political independence, and democracy even in the absence of coercion. This gap is particularly important if non-intervention is to retain its de-escalatory nature of ensuring 'that nations live in peace with one another'[64] since interventions 'threaten international peace and security'.[65]

---

[57] Ibid., Part II.B.2
[58] Tsagourias (n 10) 54.
[59] Jamnejad and Wood (n 34) 348.
[60] Ibid.
[61] Ibid.
[62] Ibid.
[63] Rosalyn Higgins, 'Intervention and international law' in Hedley Bull (ed), *Intervention in World Politics* (Clarendon Press 1984) 30.
[64] Friendly Relations Declaration (n 5).
[65] Ibid.

Yuval Shany and Dan Efrony recently performed 11 case studies on cyber operations to identify whether the rules contained in the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* had any effect on State practice and *opinio juris*.[66] While their conclusions are outside the scope of this chapter, their case studies illustrate an important, and often overlooked, lesson about coercion. That lesson is that coercion, as widely understood until now, is absent from all 11 case studies, meaning that the norm of non-intervention, in its current narrow understanding, is almost irrelevant in a world where States increasingly resort to cyber operations as a method of interference.

Nonetheless, times have changed, and the concept of coercion may lend itself to interpretation. After all, States have evolved in regard to how they carry out their sovereign prerogatives and their priorities. What intervention meant two centuries ago is unlikely to be the same today.[67]

3.3 Expanding 'Coercion'

One approach to deal with the outdatedness of coercion is to interpret it by expanding it in a way that captures the unique challenges presented by cyberspace.

Steven Barela, for example, has asserted that the release of the compromised DNC emails constituted coercion, because of its delegitimizing effect.[68] Barela argues that this form of election meddling and manipulation constitutes in itself an act of coercion.[69] This view rightly interprets coercion broadly, as a response to the diversity of threats, methods, and scale posed by new technologies. As Barela notes, coercion is a 'pivotal legal term'. the interpretation of which is critical for the determination of illegality.[70]

This view does not favour an absolute abandonment of coercion, but rather that the norm of non-intervention needs to recognize a more nuanced coercion standard that would apply to these new methods of interference. This would require an assessment by the international community of which new forms of interference would significantly jeopardize the domestic and foreign affairs of a State as to make them fall within the definition of 'coercion' and therefore wrongful under international law. In other words, the international community should be asking the same question as Quincy Wright: 'When does proper influence become illegal intervention?'[71]

---

[66] Dan Efrony and Yuval Shany, 'A rule book on the shelf? Tallinn Manual 2.0 on cyberoperations and subsequent state practice' (2018) 112 *American Journal of International Law* 583.

[67] *See* Tsagourias (n 10) 50.

[68] Steven Barela, 'Cross-border cyber ops to erode legitimacy: An act of coercion' (12 January 2017) *Just Security*, https://www.justsecurity.org/36212/cross-border-cyber-ops-erodelegitimacy- act-coercion [https://perma.cc/R6MW-S4YR].

[69] Ibid. (Barela argues that foreign actors meddling in election processes, with the intention of delegitimizing them, are committing an act of coercion because 'the disruption of a free and fair election strikes at a sine qua non for the State'. Barela asks whether 'disseminating true material can be considered coercion'. He answers that the Russian hack of the DNC could be considered coercive because releasing the hacked, authentic material was intended to manipulate 'public opinion on the eve of elections'; ibid).

[70] Ibid.

[71] Quincy Wright, 'Espionage and the doctrine of non-intervention in internal affairs' in Roland J Stanger (ed), *Essays on Espionage* (Ohio State University Press 1962) 4–5. Also see Schmitt (n 14) 8 ('Coercion is accordingly more than mere influence. It involves undertaking measures that deprive the target State of choice').

3.4 Informing Non-intervention Through Human Rights

Non-intervention may be losing its appeal in the cyber era due to a lack of understanding of how it applies in cyberspace. Human rights law may serve as a critical guidance on what values non-intervention ought to be protecting.

One such approach is exemplified by Nicholas Tsagourias, who argues that we cannot view non-intervention in isolation from the right to self-determination.[72] Self-determination, which protects the 'right to self-government',[73] ought to be protected by the prohibition on intervention.[74] As such, non-intervention ought not only to protect the government from being deprived of control, but also the peoples who constitute the legitimacy and mandate of such government.[75]

Informing non-intervention through human rights may ease the tension between a centuries-old norm, non-intervention, and technological innovation's permeation in society. Some other human rights may supplement the right to self-determination in infusing non-intervention with substance. For example, the right to privacy[76] and freedom of expression, which includes the freedom to seek, receive and impart information and ideas.[77] These rights form some of the essence of self-determination, and given that role, may further facilitate a clearer understanding of non-intervention in the cyber era.

3.5 Coercion as an Effect

Some questions that may need further consideration in light of coercion's irrelevancy to today's methods of interference are: is State-sponsored manipulation online wrongful? Would a State be in violation of non-intervention if it were to use political bots in violation of terms of service of social media platforms? Can interference through disruption be considered a prohibited intervention? Some of these questions may be answered by looking at coercion as an effect rather than method.

McDougal and Feliciano's consequentiality approach to coercion may have some significant utility on this issue. They suggest looking at coercion beyond degree of coercion, and consider elements such as 'the importance and number of values affected, the extent to which such values are affected, and the number of participants whose values are so affected'.[78] Given the substantial technological shifts globally, it may be helpful to look at coercion from the consequentiality angle, looking at the *effects* rather than the *tools and methods*.

---

[72] *See* Tsagourias (n 12).

[73] Ibid.

[74] Ibid.

[75] Tsagourias (n 10) 52.

[76] International Covenant on Civil and Political Rights (ICCPR), adopted Dec. 16, 1966, art 17 (1), G.A. Res. 2200A (XXI), U.N. GAOR, 21st Sess., Supp. No. 16, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171 (entered into force Mar. 23, 1976) (emphasis added).

[77] ICCPR, art 19(2).

[78] Myres McDougal and Florentino Feliciano, 'International coercion and world public order: The general principles of the law of war' (1958) 67 *Yale Law Journal* 771, 782.

These questions are particularly pressing given how States are already using methods of manipulation to interfere with domestic political processes.[79] The use of sophisticated manipulation techniques, usually with the help of machine learning to enhance microtargeting ability, is a major obstacle for non-intervention.[80] Manipulation through social media in a way that impairs voter's ability to autonomously reflect and rationalize individual choices may sidestep the stringent coercion requirement. For example, the Russian interference in the 2016 US presidential election and the UK referendum on the secession from the European Union (Brexit)[81] through social media herald the future of online political manipulation which does not reach the level of coercion.[82] Indeed, the Internet Research Agency spent two million dollars to promote Trump and denigrate Clinton through advertisement on social media platforms – Facebook, Twitter, and Instagram.[83] Looking at the effects relieves some of the difficulty in determining whether an act of interference is utilizing coercive methods or not.

3.6 Manipulation v. Propaganda

As acts of election interference online become more subtle and sophisticated, we are presented with the difficulty of categorizing online voter manipulation.

The difficulty of non-intervention to apply to online manipulation stems largely from a conflation of propaganda and manipulation. Propaganda, as a method of interference, is usually not illegal under international law.[84] Propaganda may become somewhat problematic if 'the audiences' choice of alternatives [is] severely restricted as a result of the use of the instruments'.[85] But manipulation is qualitatively worse. Manipulation employs sophisticated techniques to undermine the autonomy and agency of individuals by exploiting their human vulnerabilities.[86] This is further bolstered by technological tools like machine learning,

---

[79] Max Boot and Max Bergmann, *Defending America from Foreign Election Interference,* Council on Foreign Relations (6 March 2019) ('Russia is continuing to try to "wreak havoc over our elections" ... Other states and even nonstate actors will also likely seek to emulate this model').

[80] Natasha Singer, '"Weaponized ad technology": Facebook's moneymakers gets a critical eye', *New York Times* (16 August 2018) https://www.nytimes.com/2018/08/16/technology/facebook-microtargeting-advertising.html.

[81] Patrick Wintour, 'Russian bid to influence Brexit vote detailed in New US Senate Report', *The Guardian* (10 January 2018) https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report [perma.cc/4WGK-XYYJ].

[82] Craig Timberg, 'Russia used mainstream media to manipulate American voters', *Washington Post* (15 February 2018) https://www.washingtonpost.com/business/technology/russia-used-mainstream-media-to-manipulate-american-voters/2018/02/15/85f7914e-11a7-11e8-9065-e55346f6de81_story.html?noredirect=on&utm_term=.4dc6ad5a8e27 [perma.cc/9W2E-8FJS].

[83] Oliver Carroll, 'St. Petersburg "troll farm" had 90 dedicated staff working to influence US election campaign', *The Independent* (17 October 2017) https://www.independent.co.uk/news/world/europe/russia-us-election-donald-trump-st-petersburg-troll-farm-hillary-clinton-a8005276.html.

[84] Schmitt (n 18) 46 (2018) ('engaging in election propaganda does not amount to interference, at least as a matter of law. This conclusion is supported by the extensive State practice of engaging in both truthful and untruthful propaganda during foreign elections').

[85] Bhagevatula Murity, *Propaganda and World Public Order* (1968) 1.

[86] *See* Ido Kilovaty, 'Legally cognizable manipulation' (2019) 34 *Berkeley Technology Law Journal* 457, 471 ('manipulation exploits weaknesses and vulnerabilities of the subject based on data available about her. Manipulators learn these weaknesses and vulnerabilities by using advanced algorithms to analyze thousands of different data points and create a certain personality profile').

enabling this manipulation to take place at scale.[87] Manipulation exacerbates the challenges associated with propaganda. Schmitt agrees that 'manipulation of voters' ability to assess the messages in coming to their own decision tipped the scales and therefore constituted unlawful interference'.[88]

The Tallinn Manual 2.0 does not mention manipulation per se, but it does offer a distinction between coercion and 'persuasion, criticism, public diplomacy, propaganda, retribution, mere maliciousness, and the like'[89] suggesting that the latter are not in violation of non-intervention because they are not coercive. This list, however, does not include manipulation, which may not be coercive per se, but inherently includes more than State A having mere influence over State B. Although the Tallinn Manual gives a few relatively easy scenarios that do not reach the level of unlawful intervention, a few experts claimed context and consequences of an act are required to determine whether a violation occurred.[90] This disagreement is present in one example from the Tallinn Manual: State A leaks the domestic intelligence records of State B to create a political crisis within the victim State B,[91] with the result that State B adopts a policy that it would not have adopted otherwise. Drafters were split on whether State B's action was caused directly by the leak and was therefore coerced.[92] Without explicit coercion, it is debatable whether intervention occurred, which raises a host of issues for the future of non-intervention.

3.7 The Requirement of Victim State's Knowledge

The difficulty with coercion as a standard for non-intervention is further exemplified in a divide between the *Tallinn Manual 2.0* experts with respect to cyber operation designed to hack electronic ballots and whether the victim's knowledge of the operation is required for non-intervention to be invoked.[93] The majority of Tallinn Manual's experts believed this to be an act of prohibited intervention regardless of knowledge. However, a few experts argued that it would only qualify as prohibited intervention if the victim State knows of such a cyber operation.[94]

This minority view is impractical in the cyber context since victim States would rarely be aware in real time that their or their citizens' decisions are being affected by manipulation, disruption, or disinformation. Such lack of knowledge should not preclude the wrongfulness of the initial intervening cyber operation. Even Michael Schmitt subsequently admitted that the ambiguity on this question 'represents a troubling threat to the democratic process'.[95] This

---

87 Vyacheslav Polonski, 'How artificial intelligence conquered democracy', *The Independent* (15 August 2017) https://www.independent.co.uk/news/long_reads/artificial-intelligence-democracy-elections-trump-brexit-clinton-a7883911.html ('This highly sophisticated micro-targeting operation relied on big data and machine learning to influence people's emotions. Different voters received different messages based on predictions about their susceptibility to different arguments').

88 Schmitt (n 18) 47.

89 Tallinn Manual 2.0 (n 32) 318.

90 Ibid., 319.

91 Ibid.

92 Ibid., 320.

93 Ibid., 320–1.

94 Ibid.

95 Schmitt (n 18) 67.

hypothetical demonstrates the difficulty of applying coercion to a manipulation of election integrity. It is not a coercive act (do X, or else), but rather an act that deprives either the victim State or its citizens of a free choice. Though, such non-coercive deprivation of free choice could arguably constitute prohibited intervention nonetheless. As explored earlier, Nicholas Tsagourias argues that the right to self-determination may inform the scope of non-intervention's coercion element.[96] In other words, whenever one State forces its will onto another State, the latter 'loses control over a matter by subordinating its will … in such a way that it has no effective choice'.[97] This approach alleviates some of the difficulties with regard to knowledge of the victim State.

3.8 Coercion: Out. Manipulation and Disinformation: In.

A major trend in transnational interference is for interfering States to focus on swaying public opinion, sowing distrust in institutions, and political doxing. These objectives were largely exemplified by the Russian interference in the 2016 US presidential election. As the report issues by the Office of the Director of National Intelligence (ODNI Report) provided:

> Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election. Russia's goals were to undermine public faith in the U.S. democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump.[98]

The ODNI Report portrays a troubling picture – States have no interest anymore in coercing each other to pursue a policy or a choice that they otherwise would not. Interference operations can be far more successful if it were to discredit opponents and target the public faith in political (usually democratic) institutions and processes.

Schmitt agrees that the assertion that 'exfiltration of data and its weaponization through release at critical points in the election' constitutes intervention is 'somewhat supportable'.[99] This suggest that there may be some nuance with doxing and swaying public opinion through the weaponization of information that may qualify the operation as unlawful intervention.

Indeed, as former President Barack Obama was responding to Russia's interference in the 2016 presidential election, the White House identified that 'Russia's cyber activities were intended to influence the election, erode faith in U.S. democratic institutions, sow doubt about the integrity of our electoral process, and undermine confidence in the institutions of the U.S. government.'[100]

The texts of different instruments support the assertion that some propaganda may cross the line from legitimate speech to interference. For example, the 1976 Declaration on Non-Interference expressed concern about 'organized campaigns of vilification and intimidation' and 'subversion and defamation'. The 1981 Declaration on the Inadmissibility of

---

[96] See Tsagourias (n 10) 52–3.

[97] Ibid. 53.

[98] Office of the Director of National Intelligence, ICA 2017-01D, Assessing Russian Activities and Intentions in Recent US Elections (6 January 2017).

[99] Schmitt (n 18) 47.

[100] White House, Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment (29 December 2016).

Intervention and Interference goes even further, by calling on States to 'abstain from any defamatory campaign, vilification or hostile propaganda'.[101] While propaganda per se is not in violation of non-intervention, the concern expressed by both declaration illustrates that the integrity of political institutions and processes was of importance to the drafters.

Does massively swaying public opinion constitute unlawful intervention? What about making the public distrust its own institutions? These activities and their effect may be an important test for the norm of non-intervention.

3.9 The Causal Nexus Problem

The problem with today's interference techniques may also be framed in terms of causation. While many of the past acts of interference had a direct causal link between the act and the coercive outcome, technological landscape at present may allow perpetrators to design their interference acts in a way that obfuscates this direct causal link.

For example, by employing Twitter tolls/bots, State A is able to lead to a certain coercive outcome in State B without necessarily targeting State B with any *direct* coercive act targeting its *domaine réservé*. As such, the coercive outcome from the use of political bots will only take place much later in time, in a manner that disassociates this bot network from the eventual outcome. While it is clear that Russia's extensive bot network on social media and other interfering acts had a significant impact on the discourse during the presidential election of 2016, it is still unclear to what degree it affected the outcome of the election.[102] Though, the success of an act of intervention is immaterial to the lawfulness of such act, so long as it coercively targets the *domaine réservé.*

The Report on The Investigation Into Russian Interference In The 2016 Presidential Election ('Mueller Report') identified the use of bot networks to amplify propaganda, disinformation, and manipulation campaigns online.[103] The same bot network was also the subject of the Special Counsel's Office indictment against 13 Russian individuals involved in the disinformation campaigns on the eve of the 2016 presidential election.[104]

This problem overlaps with the difficulty of distinguishing State and non-State actors, as well as protected and unprotected domestic and foreign affairs. The difficulty of attribution

---

[101] Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States (A/RES/36/103) at 2(j).

[102] Philip Bump, 'Actually, the Mueller Report showed that Russia did affect the vote', *Washington Post* (19 April 2019) https://www.washingtonpost.com/politics/2019/04/19/actually-mueller-report-showed-that-russia-did-affect-vote/.

[103] *See* Special Counsel Robert S Mueller Report on the Investigation into Russia Interference in the 2016 Presidential Election (2019) 26 ('the IRA [Internet Research Agency] operated a network of automated Twitter accounts (commonly referred to as a bot network) that enabled the IRA to amplify existing content on Twitter').

[104] Department of Justice, Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System (16 February 2018):

> To hide the Russian origin of their activities, the defendants allegedly purchased space on computer servers located within the United States in order to set up a virtual private network. The defendants allegedly used that infrastructure to establish hundreds of accounts on social media networks such as Facebook, Instagram, and Twitter, making it appear that the accounts were controlled by persons within the United States.

certainly plays a major role here as well.[105] The emerging power of social media platforms is a double-edged sword, because it also makes liberal democracies immensely vulnerable if these platforms were to be misused by hostile foreign governments.

4. CONCLUSION

Election interference in the cyber era significantly challenges the norm of non-intervention. At the same time, it offers an opportunity for reconceptualization of non-intervention in light of new technologies of interference. This chapter offers some insights on the conundrum of cyber intervention. Primarily, how the two elements of non-intervention – *domaine réservé* and coercion – are outdated given the scale, reach, and interconnectedness of cyberspace. While applying existing norms and principles may be intuitive, such an approach does not necessarily work in the context of non-intervention. Expanding our understanding of coercion, informing its scope through human rights, and acknowledging the role of manipulation, disinformation, and disruption is crucial for the future of non-intervention in cyberspace.

[105] See Hollis (n 43) ('Ironically, the potential for a false flag means that a State caught red-handed can always invoke plausible deniability and suggest that they are themselves a victim as some other, unknown super-sophisticated actor is trying to frame them').

6. State responsibility in cyberspace

Constantine Antonopoulos

1. INTRODUCTION

Cyberspace is a domain the use of which is indispensable to the entire or at least a substantial part of the global population. It is a non-physical domain created by computer systems that allows people to communicate with each other, to exchange or to gather information. Moreover, it refers to the 'notional environment in which digitized information is communicated over computer networks'.[1] It would be an understatement to say that cyberspace is only important to private individuals, corporations and States; it underlines every aspect of modern society and it is both the domain where and the medium by which economic, public safety, civil society and national security activities are pursued.

While the usefulness of cyberspace is universally acknowledged, acts in the form of cyber-crime and espionage are also prevalent in it.[2] In particular, since private business and governments conduct most of their functions and activities through or in cyberspace, safety and resilience are important matters. It is, therefore, not inconceivable that cyberspace may be used in such a way as to cause harm to States or to compel them to act in a particular manner. There have been a number of episodes in State practice that have revealed how the hostile use of cyberspace may affect the orderly function of basic services in a State or threaten its security. In 2007 Estonia was the object of massive and coordinated computer hacking attacks that paralyzed its economy and the functioning of government services for weeks. In 2008 Georgia was the target of similar attacks during the conflict with the Russian Federation with respect to South Ossetia. Also, in 2009 a computer virus by the name of Stuxnet caused the progress of the nuclear program of Iran to suffer significant delay.[3] Moreover, in 2012 a computer virus was unleashed against Aramco, the State oil company of Saudi Arabia that erased data on three-quarters of its corporate PCs.[4] In June 2016 the Democratic National Committee computers were hacked (allegedly) by Russian government agents in an attempt to influence voters against Hillary Clinton, the Democratic Party candidate in that year's presidential election.[5] Last but not least, in June 2017, a piece of malware by the name of NotPetya caused extensive damage to company and bank computer networks in the Ukraine and other countries in Europe

[1] US Department of Defense, 'Dictionary of Military and Associated Terms' JP 1–02 (12 April 2001, as amended through 31 August 2005) 139.

[2] Mary Ellen O'Connell, 'Cyber security without cyber war' (2012) 17 *Journal of Conflict and Security Law* 187, 190.

[3] On these episodes see O'Connell (n 2) 192–4; Russell Buchan, 'Cyber attacks: Unlawful uses of force or prohibited interventions?' (2012) 17 *Journal of Conflict and Security Law* 211, 218–21.

[4] Nicole Perlroth, 'Cyberattack on Saudi firm, U.S. sees Iran firing back', *New York Times* (23 October 2012) https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html accessed on 22 January 2020.

[5] William Banks, 'State responsibility and attribution of cyber intrusions after *Tallinn 2.0*' (2017) 95 *Texas L. R.* 1487, 1487–92.

(notably, the Danish shipping corporation A.P. Møller-Maersk), Asia and the United States.[6] In this context the question arises whether such use of cyberspace may give rise to State responsibility. The answer must be in the affirmative provided that such use amounts to an 'internationally wrongful act'.[7] Since cyberspace is a domain where States interact, they must conduct themselves in accordance with international law[8] and, therefore, the use of cyberspace is subject to international law. As the 2013 and 2015 UN GGE Reports state, international law applies in cyberspace.[9] However, the law on international responsibility is facing substantive challenges due to the particularities of cyberspace which complexify attribution, a necessary component of the law of State responsibility. Be that as it may, the present author contends that the application of the law of State responsibility to cyberspace is not impossible because attribution can be established in certain instances and it is not impossible to establish State responsibility on the basis of a breach of the obligation of due diligence, which dispenses with the difficulty of attributing acts of individuals to a State. To claim that State responsibility in cyberspace is by definition inapplicable would amount to saying that technology creates lacunae or 'law-free zones' and gives rise to unhindered behaviour.[10]

In this chapter I will, first, briefly outline the legal framework of the law of State responsibility and focus in particular on its two main requirements namely, attribution of a wrongful act to a State and breach of an international law obligation (section 2). I will then address the challenges presented by the particular features of cyberspace to attribution and contend that attribution should be performed on the basis of rebuttable presumption (section 3). The chapter then considers the requirement of breach in particular in relation to the principle of due diligence and contends that the latter provides the most reliable way to establish State responsibility because it does away with the requirement of attribution (section 4). The chapter ends with certain concluding remarks (section 5).

---

[6] Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ accessed on 22 January 2020.

[7] The International Law Commission Articles on State Responsibility 2001 in James Crawford (ed), *The International Law Commission's Articles on State Responsibility, Introduction, Text and Commentaries* (CUP 2002) 61.

[8] O'Connell (n 2) 189.

[9] UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013) UN Doc A/68/98; UNGA, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174.

[10] Ibid. Also see Hersch Lauterpacht, *The Function of Law in the International Community* (OUP 2011) 68–77. Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution, Office of the Director of National Intelligence, Report, 6 January 2017, 2: 'The nature of cyberspace makes attribution of cyber operations difficult but not impossible. Every kind of cyber operation—malicious or not—leaves a trail'.

2. AN OUTLINE OF THE REQUIREMENTS OF STATE RESPONSIBILITY

State responsibility emerged as a branch of international law by way of private law analogy.[11] The Permanent Court of International Justice (PCIJ) ruled in *Factory at Chorzów (Indemnities)* 'it is a principle of international law, and even a general conception of law, that any breach of an engagement involves an obligation to make reparation'.[12] However, subsequent judicial pronouncements and the work of the International Law Commission (ILC) mark a departure from legal analogies with the domestic law of tort in favour of reconstructing responsibility as a matter of international public law arising when an act: (1) is attributable to a State; and (2) constitutes a breach of an international obligation. In *US Diplomatic and Consular Staff in Tehran* the International Court (ICJ) stated that it had to 'determine how far, legally, the acts in question may be regarded as imputable to the Iranian State' and whether they were compatible or not 'with the obligations of Iran under treaties in force or under any other rules of international law that may be applicable'.[13] Moreover, in *Bosnian Genocide* the ICJ ruled with regard to the breach of the Genocide Convention that 'the obligations in question … and the responsibilities of States that would arise from breach of such obligations are obligations and responsibilities under international law. They are not of a criminal nature.'[14]

The contemporary law of State responsibility has as its principal source of reference the *Articles on the Responsibility of States for Internationally Wrongful Acts* (ARS) adopted by the ILC in 2001.[15] This text is not (or not yet) a treaty. However, since 2001 it has been extensively cited by international courts and tribunals as well as in State practice and for this reason it is considered to be an authoritative statement of the customary international law on State responsibility.[16] The legal regime introduced by ARS is premised on the distinction introduced by ILC Rapporteur Roberto Ago between 'primary obligations' and 'secondary rules'. The very first paragraph of the Introduction of the Commentaries to ARS states that:

> The emphasis is on the secondary rules of State responsibility, that is to say, the general conditions under international law for the State to be considered responsible for wrongful actions or omissions,

---

[11] See generally, Hersch Lauterpacht, *Private Law Sources and Analogies of International Law* (The Law–Book Exchange 2002) Ch III, Sec VII.

[12] *The Factory at Chorzów (Claim for Indemnity) (Germany v. Poland)* [1928] PCIJ Ser A No 17, 29.

[13] *Case Concerning United States Diplomatic and Consular Staff in Tehran (USA v. Iran)* [1980] ICJ Rep 3, 29.

[14] *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* [2007] ICJ Rep 43, 115.

[15] [2001] Yearbook of the ILC, Vol. II (Part Two).

[16] [2010] UNGA Responsibility of States for Internationally Wrongful Acts – Compilation of Decisions of International Courts, Tribunals and other bodies (Report of the Secretary-General) A/65/76; [2010] UNGA Responsibility of States for Internationally Wrongful Acts – Comments and Information received from Governments (Report of the Secretary-General) A/65/96; [2013] UNGA Responsibility of States for Internationally Wrongful Acts – Compilation of Decisions of International Courts, Tribunals and other bodies (Report of the Secretary-General) A/68/72; [2016]UNGA Responsibility of States for Internationally Wrongful Acts – Compilation of Decisions of International Courts, Tribunals and other bodies (Report of the Secretary-General) A/71/80; [2019]UNGA Responsibility of States for Internationally Wrongful Acts – Compilation of Decisions of International Courts, Tribunals and other bodies (Report of the Secretary-General) A/74/83; James Crawford (ed), *Brownlie's Principles of Public International Law* (OUP 2019) 524.

> and the legal consequences which flow therefrom. The articles do not attempt to define the content of the international obligations breach of which gives rise to responsibility.[17]

A second basic feature of ARS is that it views the responsibility of States not as an exclusive pattern of bilateral relations between the wrongdoing and the injured State. Instead, State responsibility is given a public order dimension by laying emphasis on the existence of an internationally wrongful act[18] and not on the damage or injury caused on the victim. As the Commentary to Article 1 ARS states:

> the term 'international responsibility' … covers the relations which arise under international law from the internationally wrongful act of a State, whether such relations are limited to the wrongdoing State and one injured State or whether they extend also to other States or indeed to other subjects of international law, and whether they are centred on obligations of restitution or compensation or also give the injured State the possibility of responding by way of counter-measures.[19]

Moreover, this dimension of the law of State responsibility is further supported by Articles 40 and 48 ARS dealing, respectively, with serious breaches of obligations arising under a peremptory norm of international law and the invocation of the responsibility of a State by States other than the injured party.

As the emphasis in ARS lies in the wrongful act, central position is given to its requirements, namely, attribution to a State and breach of one of its international law obligations (Art. 2 ARS). Attribution means 'the operation of attaching a given act or omission to a State'[20] and to this end the ARS relies on the relationship between individuals with a particular State. As the Commentary to Article 2 ARS notes, the fact is that States act through human beings or groups; therefore, the issue of attribution is reduced to identifying the persons, groups or entities that should be considered to act on behalf of the State.[21] This finding appears to rest on a dual basis: it is either the status of a person, a group or entity that make them act on behalf of the State or the control exercised by a State over the activities of a person or a group.

It follows that the responsibility of a State is engaged for acts or omissions by the following categories of individuals:

(a) *De jure* State organs, irrespective of their hierarchical position in the apparatus of the State or the constitutional structure or organization of the State (namely, whether it is a unitary or federal State) (Art.4 ARS);
(b) *De facto* State organs, namely, non-State actors or entities that have been 'elevated' to *de facto* State agents or organs because they are under the absolute dependence and control of a State. In *Bosnian Genocide* the issue before the ICJ was whether the genocidal acts perpetrated by the Bosnian Serbs in Srebrenica could be attributed to Serbia. The Court ruled that:

---

[17] Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries [2001] A/56/10 31.

[18] The International Law Commission Articles on State Responsibility (n 7) art 1.

[19] Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries (n 17) 33.

[20] Ibid., 36.

[21] Ibid., 35.

> [t]his question has in fact two aspects, which the Court must consider separately. First, it should be ascertained whether the acts committed in Srebrenica were perpetrated by organs of the Respondent [namely, Serbia], i.e., by persons or entities whose conduct is necessarily attributable to it, because they are in fact instruments of its action. Next, if the preceding question is answered in the negative, it should be ascertained whether the acts in question were committed by persons who, while not organs of the Respondent, did nevertheless act on the instruments of, or under the direction or control of, the Respondent.[22]

The Court then proceeded to identify *de facto* States organs as:

> persons, groups of persons or entities [that], may for purposes of international responsibility, be equated with State organs even if that status does not follow from internal law, provided that in fact the persons, groups or entities act in 'complete dependence' on the State of which they are ultimately the instrument ….[23]

(c) *Delegation of Government Authority to individuals or entities.* In this case the conduct of a non-State actor (i.e., 'a person or entity which is not the organ of the State') is to be considered as an act of the State if the non-State actor 'is empowered by the law of that State to exercise elements of governmental authority' and it 'is acting in that capacity in the particular instance' (Art. 5 ARS);

(d) Acts of organs of a State placed at the disposal of another State. In this case, the acts or omissions of that organ in the exercise of government authority on behalf of the State at the disposal of which it was placed are attributed to the latter State (Art. 6 ARS);

(e) *Ultra Vires Acts.* A State organ or entity gives rise to the responsibility of the State even when acting in this capacity it exceeds its authority or against instructions (Art.7 ARS);

(f) *Instructions, Direction and Control of a State over acts of private persons*. According to the ICJ, the State must exercise 'effective control' over individuals or groups in order for their acts to be attributed to that State. The Court reached this finding in *Nicaragua* where it ruled that the US assistance to the *contras* and its general control over them were not sufficient in default of further evidence to attribute their acts of violating human rights and humanitarian law to the US government. By contrast '[f]or this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had effective control of the military and paramilitary operations in the course of which the alleged violations were committed.'[24] In *Bosnian Genocide* the Court having found that the Bosnian Serbs did not constitute a *de facto* organ of Serbia proceeded to determine whether Serbia exercised effective control over them. The Court explained that the:

> test thus formulated differs in two respects from the test … to determine whether a person or entity may be equated with a State organ even if not having that status under internal law. First, in this context it is not necessary to show that the persons who performed the acts alleged to have violated international law were in general in a relationship of 'complete dependence' on the respondent State; it has to be proved that they acted in accordance with the State's instructions or under its 'effective

---

[22] *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 14) 201.

[23] Ibid., 205 (emphasis added).

[24] *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. USA)* (Merits) [1986] ICJ Rep 14, 64–5.

> control'. It must however be shown that this 'effective control' was exercised, or that the State's instructions were given, in respect of each operation in which the alleged violations occurred, not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations.[25]

In this respect, the Court declined to uphold the ruling of the ICTY Appeals Chamber in the *Tadić* case where the ad hoc Tribunal applied the test of 'overall control' that dispenses with the need to evaluate control of a State over each specific operation of a non-State actor;[26] the Court took the view that the determination of State responsibility on the part of Serbia did not constitute an indispensable finding to determine individual criminal responsibility by an international criminal tribunal[27] (Art. 8 ARS);

(g) *Exercise of elements of government authority in the absence of or inadequate function of State authorities and in circumstances that warrant the exercise of this authority*. In *Yeager v. Islamic Republic of Iran* the Iran-US Claims Tribunal ruled that the immigration, customs and other similar acts that had been carried out by the Revolutionary Guards at the Tehran airport in the immediate aftermath of the Islamic revolution were attributable to Iran. The Tribunal reasoned that even though these functions were not authorized by the Iranian government they objectively consisted in the exercise of elements of governmental authority in the absence of official authorities of the State 'in operations of which the new Government must have had knowledge and to which it did not specifically object.'[28] (Art. 9 ARS);

(h) The acts or omissions of an insurrectional or other movement are attributed to a State in the event the insurrection is successful and the movement becomes the government of the State (Art. 10 ARS);

(i) *Approval and Adoption by a State of acts of private persons or entities.* In *US Diplomatic and Consular Staff in Tehran* the Court ruled that the act of overrunning of the US Embassy in Tehran by demonstrators and the seizure as hostages of the US diplomatic staff could not be as such attributed to the Iranian Government because the demonstrators were neither State organs nor did they carry out a specific government act on behalf of the State[29]. However, the responsibility of Iran for the acts of the demonstrators was established at a later stage when the Iranian government approved of and adopted the occupation of the Embassy premises and the captivity of the US diplomatic staff as its own[30] (Art.11 ARS).

The second requirement of State responsibility, namely a breach of an international obligation, may consist of a physical act or an omission and may emanate from an existing rule of

---

[25] *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 14) 211–5.

[26] *Prosecutor v. Tadić*, ICTY Appeals Chamber Judgment, Case No. IT–94–1–A [1999] para 145; but *cf* ibid., paras 118–22, where the Tribunal has drawn a distinction between acts performed by private individuals to which the effective control test applies (as articulated in the *Nicaragua Case*) and organized military groups to which the overall control test applies.

[27] *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 14) 209–10.

[28] [1987] 17 Iran–US Claims Tribunal Rep, 104.

[29] *Case Concerning United States Diplomatic and Consular Staff in Tehran* (n 13) (Merits) 29–30.

[30] Ibid., 33–6.

customary law or treaty law (Art. 12 ARS). Moreover, the responsibility of a State may arise regardless of whether the wrongful act is momentary or continuous (Arts 14 and 15 ARS) and irrespective of whether it constitutes part of a composite activity. Furthermore, State responsibility arises with respect to acts of another State. This is not to say that the acts of that other State are attributed to the former State for, as the ILC has made clear, the ARS is premised on the principle that 'each State is responsible for its own wrongful conduct … attributable to it … which is in breach of an international obligation of that State …' and that 'responsibility is specific to the State concerned'.[31]In this respect it should also be stated that even if the ILC had identified instances of 'collaborative conduct'[32] it has not introduced a particular legal framework of 'shared responsibility' but views the collaborative element as a factual rather than a normative parameter.[33] This is further corroborated by Article 47(1) ARS on the invocation of State responsibility for an internationally wrongful act committed by a plurality of States: in this instance it is again the responsibility of each State that can be invoked with respect to this act albeit separately. Having said this, the responsibility of a State for the acts of another State arises in cases of aid or assistance, direction and control and coercion. In each of these cases two requirements need to be fulfilled cumulatively: first, the conduct must be internationally wrongful if it were committed by the aiding/controlling/coercing State and, secondly, the aiding/controlling/coercing State must have knowledge of the circumstances of the internationally wrongful act (Arts 16–18 ARS). Finally, the ARS provide for grounds precluding the wrongfulness of an act that prima facie constitutes a breach of an international obligation; these are: consent (Art. 20), self-defence (Art. 21), countermeasures (Arts 22, 49–54), *force majeure* (Art. 23), distress (Art. 24) and necessity (Art. 25).

3. ATTRIBUTION IN CYBERSPACE

Cyberspace as a domain and the use of electronic devices as a medium of State conduct raises difficulties with respect to ascribing particular acts to States.[34] There is no reason to sweepingly deny as a matter of principle the application of the rules of attribution provided in ARS to conduct in cyberspace. However, their application in general[35] and the identification of individuals or entities, in particular, that operate in cyberspace is characterized by considerable difficulty, for cyberspace guarantees a large measure of anonymity or deniability. Thus, it is extremely difficult to identify directly and with certainty the person or entity operating a personal computer. Identification of persons, and by consequence, attribution is *prima facie* possible via the identification of a computer by way of its IP that identifies its precise location.

Therefore, an internationally wrongful act in cyberspace appears to be ascribed to a particular computer whereas the identity of the person operating it may be established either by way of presumption or on the basis of inside information disclosed by government agents of the

---

[31] Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries (n 17) 64.

[32] Ibid.

[33] On shared responsibility see generally André Nollkaemper and Dov Jacobs, 'Shared responsibility in international law: A conceptual framework' (2013) 34 *Michigan J of Intl L* 359.

[34] Nicholas Tsagourias and Michael Farrell, 'Cyber attribution: Legal and technical approaches and challenges' (2020) 31 *European Journal of International Law* 941.

[35] Ibid., 953–55.

State perpetrating the internationally wrongful acts in cyberspace[36]or by way of intelligence based on State agencies acting alone or in cooperation or by cyber security companies acting alone or in cooperation with State agencies.[37] However, States tend to treat the attribution process as their prerogative.[38] Thus, even though in a number of serious hostile acts in cyberspace attribution to particular States was established by private companies in relatively short time, it has taken governments much longer to do so. In the case of the cyber attack against the DNC during the US presidential election of 2016, the hostile activity was first attributed to Russia by a private internet security firm but it has taken the US government six months to reach its own conclusions on attribution.[39] This does not mean that governments ignore the evidence collected by private firms but they want to make their own assessment of the evidence and make their own determination. In fact, governments take into account evidence from the private sector in making their own assessments. In February 2013 the private cyber-security firm Mandiant (present Fire Eye) published a report in which it identified Unit 61398 of the Chinese People's Liberation Army as the perpetrator of 141 unlawful cyber acts against various US companies; on the basis of this information a grand jury in the Western District of Pennsylvania indicted five members of the Chinese Army.[40]

Having said that and moving to the modes of attribution, if a computer is identified by way of its location (in the premises of a government department or a diplomatic mission) as a government computer then the malicious operation may in principle be attributed to that particular State. This would be the case either because of the identity of the operator who is presumed to be a governmental agent or because of the mere location of the computer as this falls under the exclusive and complete control of a State. Thus, in October and November 2013 the German government launched strong diplomatic protests with the US and UK governments for allegations of electronic surveillance of German governmental departments, including the German Chancellor's Office, from the US and UK embassies in Berlin. In particular, the German government warned the UK ambassador that the interception of German government information by intelligence services from a diplomatic mission constitutes a breach of international law.[41]

---

[36] Viz., the information disclosed by the former US National Security Agency (NSA) Edward Snowden on the NSA surveillance of many foreign government agencies; 'NSA Files: Decoded', *The Guardian* (1 November 2013) https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 accessed on 20 April 2020.

[37] John P Carlin, 'Detect, disrupt, deter: A whole government approach to national security cyber threats' (2016) 7 *Harvard National Security* Journal 391, 409, 410–4; Kristen E Eichensehr, 'Decentralized cyberattack attribution' (2019) 113 *American Journal of International Law Unbound* 213.

[38] United Kingdom Attorney General's Office, *Cyber and International Law in the 21st Century* (23 May 2018) https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century; République Française, Ministère des Armées, *Droit International Appliqué aux Opérations dans le Cyberespace* (2019). Karine Bannelier and Théodore Christakis, *Cyber-Attacks. Prevention-Reactions: The Role of States and Private Actors*, Les Cahires de la Revue Défense Nationale (2017) 46.

[39] Banks (n 5) 1488–92.

[40] This is a case of attributing an internationally wrongful act to another State by way of indicting its agents; Chimène I Keitner, 'Attribution by indictment' (2019) 113 *American Journal of International Law Unbound* 207.

[41] Nigel Morris and others, 'Germany calls in Britain's ambassador to demand explanation over "secret Berlin listening post"', *The Independent* (6 November 2013) http://www.independent.co.uk/news/uk/politics/germany–calls–in–britains–ambassador–to–demand–explanation–over–secret–berlin–listening–post–8923082.html accessed 20 April 2020.

The Tallinn Manual which relies heavily on the ARS adopts, however, a rather cautious approach to attribution in such cases by stating that the fact that a cyber operation has its source in government cyber infrastructure is not sufficient to attribute these acts to a State; it merely constitutes an *indication* that a particular State is associated with the cyber operation. The Manual explains this approach by reference to the particular features of the cyberspace and especially the likelihood that a government cyber infrastructure may have been 'hijacked' by non-State actors.[42] Moreover, the former Legal Advisor of the US Department of State has acknowledged the problem of attribution in that cyberspace 'significantly increases an actor's ability to engage in attacks with "plausible deniability", by acting through proxies' and suggested that this challenge is 'as much questions of a technical and policy nature rather than exclusively or predominantly' a question of law.[43] But attribution *is* predominantly a question of law and it is not determined 'on the mere recognition of a link of factual causality'.[44] Furthermore, neither the Tallinn Manual nor the US government appear to propose an alternative framework of attribution but leave the whole issue surrounded in ambiguity which suggests a wide margin of discretion on the part of an injured State to decide the matter of attribution on the basis of extra-legal factors, such as the general political climate between it and another State.[45] In the absence of an alternative proposition, it appears that they are in favour of a more flexible application of the current legal framework of attribution by an injured State on a case-by-case basis.

Attribution of a wrongful act to a State is also a matter of evidence. As malicious acts in cyberspace emanate from computers located in the territory of one or more States, the territorial location of computers may serve as a starting-point. State sovereignty entails the expectation that every State exercises control over cyber infrastructure and activities within its territory.[46] However, as the ICJ ruled in the *Corfu Channel* case the mere fact of existence of objects constituting a source of injurious acts (in this case computers engaged in injurious cyber acts) within its territory is not sufficient to impute knowledge of these acts to the State. At the same time, the victim-State is permitted 'a more liberal recourse to inferences of fact and circumstantial evidence'.[47] This lower standard of evidence was admitted in *Corfu Channel* because the UK did not have direct access to evidence and this in the context of a dispute where there was no controversy either over the territorial source of the injurious act (the territorial sea of Albania) or the agency (the mines) through which this act materialized. In the cyber context the establishment of the exact and actual source of the injurious act

---

[42] Michael N Schmitt (ed), *Tallinn Manual2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) 87–104.

[43] Banks (n 5) 1493–4; William C Banks, 'The bumpy road to a meaningful international law of cyber attribution' (2019) 113 *American Journal of International Law Unbound* 191.

[44] Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries (n 17) 38–9. Technical attribution consists of the forensic investigation into a particular cyber incident and it does have a fundamental contribution in identifying its origins; but it does not suffice by itself to determine the perpetrator and his/her precise attachment to a State.

[45] *Cf* Nicholas Tsagourias, 'Cyber attacks, self-defence and the problem of attribution' (2012) 17 *Journal of Conflict and Security Law* 229, 233.

[46] Tallinn Manual 2.0 (n 42) 30–2; Bannelier and Christakis (n 38) 13.

[47] *Corfu Channel Case (UK v. Albania)* (Merits) [1949] ICJ Rep 4, 18; also see Tallinn Manual 2.0 (n 42) 40–41. Also see Tsagourias and Farrell (n 34) 957–58, where the authors stress the importance of circumstantial evidence but always in conjunction with primary evidence.

is extremely difficult to locate, let alone establish the identity of the perpetrator.[48] Thus, it appears that a very liberal approach to evidence is called for by the very nature of cyberspace that would combine government and private intelligence gathering, expert technical knowledge, press reports[49]and (where available) revelation by defector public officials of a State (the US NSA surveillance activities were revealed by former NSA official Edward Snowden) even though the fact of defection may diminish its probative value as evidence contrary to the interests of his own State.[50]

There is a widely shared view in the literature that evidence of attribution of internationally wrongful cyber acts need not substantiate absolute certainty about the identity of the State responsible for the wrongful acts. While it is asserted that attribution must not be arbitrary,[51] at the same time it is argued that it should not be corroborated by definitive intelligence and that 'the failure to offer persuasive evidence of State attribution is not wrongful legally'.[52] This appears to be supported in State practice. While States tend not to adopt the attribution findings of private entities unreservedly and prefer to conduct their own investigation of the matter, when they make attribution statements there is hardly any evidence provided beyond mere assertion. Thus, the government of the UK attributed the NotPetya malware attack to the Russian Federation in these terms: 'The UK Government judges that the Russian Government, specifically the Russian military, was responsible for the destructive NotPetya cyber-attack of June 2017.'[53]

All the above indicate the difficulties in identifying a single State as the source of a malicious cyber act[54] which appears to leave the victim-State with two possible options: either identify the perpetrating State on the basis of the existing political climate between them or cooperation with other States in the context of international organizations or bilaterally and multilaterally or cooperation with private entities. The first avenue may entail a degree of arbitrariness and ultimately it does not, and cannot by itself, establish responsibility in the absence of more objective evidence. By contrast, the second avenue offers a better potential of identifying the alleged wrongdoing State. The fact, however, remains that such identification constitutes to a large extent a very flexible approach to the established legal framework of attribution.

---

48 Tsagourias (n 45) 233–5.

49 *Cf Nicaragua* (n 24) 40–41.

50 Ibid., 43.

51 Bannelier and Christakis (n 38) 14–15, 45–6.

52 Banks (n 5) 1499. Michael N Schmitt and Liis Vihul, 'Proxy wars in cyberspace: The evolving international law of attribution' (2014) 1 *Fletcher Security Review* 54, 64. *Cf* Lorraine Finlay and Christian Payne, 'The attribution problem and cyber armed attacks' (2019) 113 *American Journal of International Law Unbound* 202, 205–6. *Cf* Bannelier and Christakis (n 38) 13, 14–5. Tsagourias and Farrell (n 34) 966 suggest that the 'preponderance of the evidence' as an acceptable standard of proof for proving attribution.

53 Foreign Office Minister Condemns Russia for NotPetya attacks (15 February 2018) https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks accessed 23 January 2020. Equally, States against which claims of attribution are made insist that the evidence that is presented is unequivocal with regard to their involvement. Thus, Russia disputed the probative value of the evidence invoked by the US for the DNC hack and insisted on the production of hard proof of her alleged involvement. See Tsagourias and Farrell (n 34) 14.

54 Tsagourias mentions that the cyber attack on Estonia in 2007 'involved a large botnet of approximately 85,000 hijacked computers from around 178 countries': Tsagourias (n 45) 233.

The best approach in my opinion is to attribute hostile cyber acts to a State on the basis of a presumption of responsibility which may be rebutted by the State on the basis of evidence. In other words, attribution may rest on a presumption that introduces a reversal of the burden of proof. This submission departs from the ruling of the ICJ in *Corfu Channel* but unlike sea-mines computers are ubiquitous and by their nature not injurious. Thus, all that has to be established is their location in the territory of a particular State and the latter's alertness by the victim to the fact that injurious cyber acts emanate the reform. Once this takes place knowledge of the injurious activity is established. It is true that the State from the territory of which the injurious acts emanate may not constitute their actual source, as the computers on its territory may have been hijacked and constitute a 'botnet'. But this is no reason to deny the right of the victim to alert the territorial State and demand measures on its part for the cessation of the injurious activities. Such measures may entail, depending on the circumstances, a degree of denial of Internet services throughout the territory of that State, and it is a question of balancing the interests of both the victim-State and the territorial State on whether or not this is feasible.[55] However, this cannot be *prima facie* excluded as a possibility in view of the fact that States in other circumstances (for instance, when facing unrest by dissident political groups) are all too prepared to adopt sweeping measures of Internet service-denial even throughout their territories. Having said this, there appears to be only one situation in which injurious cyber acts may not be imputed to the territorial State, namely, where the acts emanate from a location that is under the exclusive jurisdiction of another State, such as the premises of a diplomatic mission or the installation of a military base.[56] In the context of the US NSA electronic surveillance practices it was reported that special units located on the rooftops of a number of US embassies in Europe and Asia (such as the US embassies in Athens and Baku) collected data.[57] In these cases these acts would not be attributed to the host States (respectively, Greece and Azerbaijan) but to the USA.

4. BREACH OF AN INTERNATIONAL OBLIGATION IN CYBERSPACE

There is no difficulty with the proposition that activities in cyberspace may constitute breach of international obligations giving rise to State responsibility. Thus, certain acts may violate the sovereignty of another State or other States, in the sense of interfering in areas of competence that are exclusively reserved to every State. This may be relative to incidents of electronic surveillance of, or espionage against, government departments and personnel of another State.[58] However, there is no consensus on this issue: according to a school of thought that relies on the famous (or infamous?) *Lotus* principle,[59] espionage is not prohibited or regulated by international law; therefore, its practice does not as such constitute a breach of the sovereignty of another State, unless perhaps some additional damage is caused.[60] On

---

55 Tallinn Manual 2.0 (n 42) 41–2.
56 Ibid., 32–3.
57 Morris (n 41).
58 On cyber espionage and international law see Buchan and Navarrete (Ch 11 of this Handbook).
59 *The Case of the 'S.S. Lotus' (France v. Turkey)* [1927] PCIJ Ser A No 1018.
60 Tallinn Manual 2.0 (n 42) 25, 323.

the other hand, it is argued that if an act is not expressly prohibited by international law this does not lead necessarily and automatically to its permissibility;[61] espionage, in particular, is practiced extensively by States but no government has ever asserted that it constitutes a lawful enterprise.[62] Moreover, cyber acts may constitute instances of unlawful intervention in the internal or external affairs of another State, provided the element of 'coercion' exists,[63] or use of force.[64]

However, as was said, a breach presupposes attribution which is rather difficult in cyberspace. This points to another and perhaps in some cases the only ground for establishing responsibility: the violation of the duty of due diligence arising from the principle that no State may knowingly allow its territory to be used for, or be the source of, acts injurious to other States.[65] The need for attribution in this case is made redundant because the breach involves an omission to act as required by a primary obligation which can be established by the fact that the State has the capacity to act to prevent such malicious acts from happening through its organs or *de facto* agents or private parties to whom government authority has been delegated. Due diligence is thus the primary obligation whose breach (failure to act or omission to act) ensures the observance of other primary obligations (based on treaty or customary law). The precise content and scope of due diligence varies in conjunction with specific obligations. The ILC has deliberately refrained from including due diligence in the Articles on State Responsibility because this would entail examination of the content of primary rules; nevertheless, it did point out that there is a presumption that any primary rule contains a qualification of due diligence.[66]

In the context of trans-boundary harm from hazardous activities the ILC has adopted the view that the duty of due diligence does not extend to guaranteeing that significant harm is to be totally prevented if it is impossible to do so. Furthermore the ILC stated that the standard of due diligence to assess the conduct of a State would be that which would be deemed 'appropriate and proportional to the degree of risk of trans-boundary harm in the particular instance'.[67] Moreover, the Sea Bed Disputes Chamber of the International Tribunal of the Law of the Sea (ITLOS) ruled in its Advisory Opinion in the *Responsibilities and Obligations of States with respect to Activities in the Area* that due diligence is a 'variable concept' and the standard it

---

[61] *Accordance with International Law of the Unilateral Declaration of Independence in respect of Kosovo, Advisory Opinion of 22 July 2010,* (Declaration of Judge Simma) [2010] ICJ Rep 403, 478–9.

[62] Anne Peters, 'Surveillance without borders? The unlawfulness of the NSA–panopticon, Part I' (1 November 2013) *EJIL: Talk!*, http://www.ejiltalk.org/surveillance–without–borders–the–unlawfulness–of–the–nsa–panopticon–part–i/ last accessed 17 November 2020.

[63] *Nicaragua* (n 26) 107–8; Tallinn Manual 2.0 (n 42) 317 et seq.; Buchan (n 3) 221–6; Nicholas Tsagourias 'Electoral cyber interference, self-determination, and the principle of non-intervention in cyberspace**'** in Dennis Broeders and Bibi Van den Berg (eds), *Governing Cyberspace: Behavior, Power and Diplomacy* (Rowman & Littlefield Publishers, 2020) 45–63.

[64] Tallinn Manual 2.0 (n 42) 328 et seq.; Tsagourias (n 45) 230–33; *cf* O'Connell (n 2) 191–2, 198–203.

[65] *Corfu Channel* (n 47) 22.

[66] Report of the International Law Commission on the work of its 51st session (Supplement No 10, 3 May–23 July 1999) GAOR, A/54/10, 86; Jan A Hessbruegge, 'The historical development of the doctrines of attribution and due diligence in international law' (2004) 36 *New York University Journal of International Law and Politics* 265, 275.

[67] ILC Draft Articles on the Prevention of Trans–Boundary Harm from Hazardous Activities (2001) A/56/10, 154.

may set may change as a result of scientific and technological developments as well as the risks involved in a particular activity.[68]

In the human rights field the duty of due diligence has been upheld in *Velasquez-Rodriguez* in which the Inter-American Court of Human Rights interpreted the obligation introduced in Article 1(1) of the Inter-American Convention of Human Rights to respect and ensure the exercise of the rights enshrined in the Convention. The Court ruled that the obligation to 'ensure' the exercise of these rights gave rise to the duty of contracting States to organize the governmental infrastructure in such a way so as to ensure 'free and full enjoyment' of the rights and prevent, investigate and punish their violation; this obligation to 'ensure' is not fulfilled solely by the existence of 'a legal system designed to make it possible to comply with this obligation – it also requires the government to conduct itself so as to effectively ensure the free and full exercise of human rights'.[69]

The ICJ has dealt with the duty of diligence in a number of disputes involving alleged breaches of international obligations in a variety of contexts. In *Corfu Channel* the Court ruled at the outset that the mere existence of the source of an injurious act (in this case the mines) in the territory of Albania was not sufficient to attribute this act to the State, for the control exercised by a State over its territory as a result of sovereignty does not establish *prima facie* knowledge of every activity taking place therein.[70] After establishing knowledge by Albania of the laying of mines in its territorial sea,[71] the Court ruled that the responsibility of Albania lay in her failure to notify the existence of a minefield in its territorial sea to third-State shipping. In the opinion of the Court, this obligation rested on three general principles, namely, elementary considerations of humanity, the freedom of maritime communication and 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'.[72] But the Court also took account of the particular factual circumstances of the case in order to confirm its legal finding: it acknowledged that if the mines had been laid at the last possible moment, namely, less than 24 hours before the UK warships struck them it would have been difficult or even impossible to issue a general notification to third-State shipping. But, as the incident took place at a time by which the Albanian authorities could have had knowledge of the existence of the mines as a result of their close surveillance of the Corfu Strait, Albania did not observe its duty of due diligence.[73] In *US Diplomatic and Consular Staff in Tehran* the Court ruled that the acts of the demonstrators who took over the premises of the US embassy and held its staff hostage could not be imputed per se to the government of Iran. However, Iran bore responsibility because of its failure to observe its obligation under the Vienna Convention on Diplomatic Relations (1961) to protect the inviolability of the persons and premises of another State's diplomatic mission.[74]

In *Congo v. Uganda* the Court dealt with Uganda's allegation that the Congo had violated its obligation of due diligence (or duty of vigilance) by failing to prevent the action of dis-

---

[68] *Responsibilities and Obligations of States Sponsoring Persons and Entities with respect to Activities in the Area* (Advisory Opinion) [2011] ITLOS Sea Bed Disputes Chamber, paras 111, 117.

[69] *Velasquez–Rodriguez v. Honduras* (Judgment of 29 July 1988) [1988] Inter–Am. Ct. HR (Ser C) No 4, paras 166–167.

[70] *Corfu Channel* (n 47) 18.

[71] Ibid., 18–22.

[72] Ibid., 22.

[73] Ibid., 22–3.

[74] *Case Concerning United States Diplomatic and Consular Staff in Tehran* (n 13) 30–33.

sident armed bands against Uganda from its territory. The Court ruled that the existence and toleration of armed groups on Congolese territory could not be assimilated with active support to these groups; in addition, the Court took into account the inimical geographical terrain where the groups operated and the material inability of the Congolese (as well as the former Zairian) government to effectively control that part of the territory of the State. Thus, the Court concluded that it cannot uphold the allegation of breach of the duty of vigilance on the part of the Congo.[75]

Moreover, in *Bosnian Genocide* the Court dealt with the obligation to prevent genocide that is enunciated in the 1948 Genocide Convention.[76] In the course of its reasoning the Court made some statements of principle regarding the duty to prevent (due diligence) even though it made it clear that it did not intend to introduce a general framework of universal application on the duty of due diligence; it observed that 'the content of duty to prevent varies from one instrument to another, according to the wording of the relevant provisions, and depending on the nature of the acts to be prevented'.[77] Then the Court analysed the content of the duty to prevent in relation to the crime of genocide. It stated at the outset that this duty was an obligation of conduct and not of result; hence, a State did not have the obligation to succeed in preventing genocide 'whatever the circumstances' but was under the obligation to 'employ all means reasonably available' to it to prevent the commission of the crime.[78] Thus, failure to achieve the desired result does not give rise to responsibility; by contrast, responsibility arises in case of manifest failure to take all steps within its power that would contribute to preventing genocide because 'in this area the notion of "due diligence", which calls for an assessment *in concreto*, is of critical importance'.

Various parameters operate when assessing whether a State has duly discharged the obligation concerned.[79] The Court proceeded to identify those parameters in relation to the specific obligation to prevent genocide and found of particular importance the capacity to influence (within the limits of the law) the perpetrators on the basis of: (a) the geographical distance between the State concerned and the scene of the crime; and (b) the strength of political or other links between the State and the perpetrators.[80] The essence of due diligence lies, therefore, in the application of all means at the disposal of the State even if may be proved on the basis of evidence to be futile; in other words a State must not be inert even in the knowledge that its measures will in all probability be ineffective to prevent the injurious act.[81] Even though the Court found that the duty to prevent genocide would give rise to responsibility only when the crime was actually committed (*viz.* Art. 14(3) ARS) it recognized that a State was not absolved from responsibility if it remains inactive until commission of the crime commences where there is a serious risk of its commission; in such a contingency the State is under the

---

[75] *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (Merits) [2005] ICJ Rep 168, 268.

[76] Convention on the Prevention and Punishment of the Crime of Genocide (1948) 78 UNTS 277, Art 1.

[77] *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 14) 220–21.

[78] Ibid., 221.

[79] Ibid.

[80] Ibid.

[81] Ibid.

obligation to employ the means available to it to prevent the crime, otherwise the substance of the obligation would be negated.[82]

Finally, in *Pulp Mills* the Court ruled that both litigants (Argentina and Uruguay) were under an obligation of due diligence to act through the Administrative Commission of the River Uruguay (CARU) with respect to adopting measures to preserve the ecological balance of the river by virtue of Article 36 of the Statute of the River Uruguay of 1975.[83] The present author submits that State responsibility as a result of breach of the duty of due diligence is consummated in the conduct of a State consisting in its failure to act and it does not extend to the end result that occurred as a consequence of this failure and that constitutes breach of a different primary rule (for instance, the prohibition of the use of force). The latter would require further evidence that the ultimate outcome was the direct result of acts or omissions amounting to the breach of this other primary rule and not simply the failure to adopt preventative measures that even they might not guarantee beyond all doubt that the end result would not occur.

On the basis of the preceding analysis it is submitted that the responsibility of a State for internationally wrongful acts in cyberspace may be established on the basis of the customary law duty of due diligence of not knowingly allowing its territory to be the source of acts violating the rights of other States. In cyberspace, the duty of due diligence is applied as a duty of vigilance rather than a duty of prevention. It also applies to any party that is the perpetrator of a malicious cyber operation (namely, a State or non-State actor) and it applies throughout the territory of the 'territorial State'.[84] Moreover, if the 'territorial State' is simply a 'transit' State then a duty of due diligence exists for this State if it has knowledge of a wrongful operation that reaches the requisite threshold of harm and is in a position to take feasible measures to thwart this operation.[85]

The content of due diligence must be assessed by taking into account, first, that the use of the Internet is not unlawful per se; secondly, that transmission from a computer or a host of computers may or may not be the actual source of the injurious activity; and, finally, that the existence of thousands of computers on the territory of a State does not by and of itself constitute knowledge of such injurious activity. Furthermore, the wrongful cyber act must be contrary to the rights of the victim-State under international law and, secondly, have serious adverse consequences.[86] This will not be the case when the cyber operation simply affects the interests of a State, or causes inconvenience or minor disruption or when a non-State actor (e.g., a blogger) publishes information that is not favourable to the target (victim) State. At the same time physical injury to persons or objects is not necessary.[87]

Regarding the requirement of knowledge, it may be either actual (when government services detect a cyber operation) or constructive when a State 'in the normal course of events would become aware of such activity'.[88] Knowledge can be established only upon the notification by the victim-State that has the discretion to identify the State or States (they may be many) from the territories of which the malicious cyber transmissions occur.

---

82 Ibid., 222.
83 *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Judgment [2010] ICJ Rep 14, 77.
84 Tallinn Manual 2.0 (n 42) 30–33.
85 Ibid., 33.
86 Ibid., 34.
87 Ibid., 36–9.
88 Ibid., 40–2.

Once knowledge is established then the territorial State is under an obligation to notify other States of the injurious acts emanating from their territory[89] and to employ 'all measures that are feasible in the circumstances', namely, all measures reasonably at their disposal to stop the wrongful cyber activity.[90] Such measures appear to be commensurate with the possession of technological capabilities to deny temporarily Internet service either to particular users or throughout the State, but it has been suggested that there is no obligation to adopt general preventive measures (as these may give rise to violations of human rights obligations) or measures that may disproportionately affect the function of the governmental and economic infrastructure of the State.[91] Thus, total denial of service is not in principle to be regarded as a reasonable response to injurious cyber acts. What is important is that a State that is established to have knowledge of injurious cyber acts emanating from its territory is under a duty to act irrespective of the fact that the said cyber activity may also originate from the territories of other States. To say that the failure to employ measures within that State's capability is of no consequence because the wrongful cyber activity also emanates from computers located in a plurality of States does not absolve the former from responsibility under due diligence. The ICJ ruled in *Bosnian Genocide* that such an assertion is irrelevant to the breach of an obligation of conduct warranted by the duty of due diligence, especially when there is a possibility of cooperation through concerted action in a situation where the perpetrator of an injurious cyber act takes over a large number of computers situated in a plurality of States.[92] Indeed, it is because of this contingency, so frequent in practice, that cooperation and concerted action is essential either on an ad hoc basis to counter specific wrongful cyber activities or on a more permanent basis through institutionalized mechanisms or a pre-existing framework of good practices in cyber-space.[93] Thus, the NATO initiatives on information security are in principle steps in the right direction[94] as well as the initiative of China and the Russian Federation for the introduction of an International Code of Conduct for Information Security.[95]

5. CONCLUSION

Cyberspace poses many challenges to the law of State responsibility as it has evolved through State practice, judicial decisions and the work of the ILC culminating in the 2001 ARS. Cyberspace as a domain has international dimensions; therefore, it is in principle amenable to regulation by international law and the rules on State responsibility will apply. Whilst a breach of an international obligation may be established without much difficulty in relation to certain

---

89 *Corfu Channel* (n 47) 22.

90 Tallinn Manual 2.0 (n 42) 47; Bannelier and Christakis (n 38) 21–2.

91 Tallinn Manual 2.0 (n 42) 44–5; Bannelier and Christakis (n 38) 20.

92 *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 14) 221.

93 O'Connell (n 2) 206–9.

94 NATO, 'NATO and Cyber Defence' (17 March 2020) http://www.nato.int/cps/en/natolive/topics_78170.htm? last accessed 20 April 2020.

95 Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary–General, Annex, UN Doc A/66/359.

types of cyber activity, it is attribution that raises difficulties that seem to defy the rules on attribution established in the ARS.

These rules are centred on acts of persons and their imputation to a particular State and the process of attribution is a juridical one. However, the nature of cyberspace as a domain, the freedom and the prima facie lawfulness of its use, the transmission of information through computers and the anonymity of the users appear to leave little scope for establishing with a relative degree of certainty the identity of the user and his/her link to a specific State. The only fact that can be established with certainty is the location of a particular computer or computers in the territory of a certain State or States. This gives rise to the presumption that the State from the territory of which cyber injurious acts emanate could be the one that may incur responsibility. However, this does not dispense with the specific rules of attribution and the fact that computers situated in the territory of a State may have been 'hijacked'. Hence there have been suggestions of overcoming this difficulty by addressing attribution more flexibly or even by going beyond its existing legal framework and placing it within the context of political relations between the States concerned. Whereas political relations may constitute a factor that the victim State may take into consideration in the attribution process, it should not substitute the existing rules on attribution and should not dispense with the burden of proof. Attribution requires evidence and due to the difficulties in collecting evidence from the territory of another State, circumstantial evidence may be admissible (for instance, the revelation in the press by former government agents that a State has engaged in wrongful cyber acts) and the burden of proof may be reversed and fall upon the State allegedly perpetrating injurious cyber acts. That said, States have recourse to information and attribution determinations by private entities, while there is close cooperation and coordination between governmental agencies within States and among States when making attributions.

That does not remove the difficulties in applying the existing rules on attribution, but such difficulties can be overcome by focusing on the primary rule breached (namely, the specific international obligation) in conjunction with the duty of due diligence either as a primary obligation (e.g., the duty to prevent genocide) or as a general principle of international law that no State must knowingly allow its territory to be used for injurious acts against other States. In this manner, responsibility may be established on the basis of knowledge that certain wrongful cyber acts have their source in computers located in the territory of a State or a plurality of States. This knowledge would be established on the basis of notification of the wrongful activity by the victim-State whereas responsibility would arise if the territorial State fails to employ feasible measures at its disposal to supress that activity.

7. Cyberspace and human rights

David P. Fidler

1. INTRODUCTION

As policy areas, cyberspace and human rights are intertwined. Understanding one requires sustained attention to the other, even though human rights do not depend on any technology and the technologies producing cyberspace have no 'hard wired' ideology. The relationship between cyberspace and human rights was forged during a unique historical moment but has exhibited increasing controversy as power and ideas have shifted in world politics. Early visions of cyberspace as an unprecedented realm for advancing human rights have given way to proliferating struggles to protect rights in a world dependent on cyber technologies but subject to diverging interests, incompatible ideas, and intensifying geopolitical competition.

The chapter begins by arguing that the Internet is the most consequential communication technology of the human rights era (Part 2). The Internet's importance to human rights is a function of chronology as much as technology. This largely American innovation became a phenomenon in a post-Cold War world dominated by US power, interests and ideology, including US perspectives on democracy, markets and human rights.

The human rights consequences of the Internet's advent are apparent in two contexts. First, cyberspace challenges general principles of international law important for human rights, including sovereignty, non-intervention and jurisdiction (Part 3). Second, cyberspace emerged into the human rights regime—the international law, institutions and processes built to protect human rights (Part 4). The human rights 'footprint' of cyberspace is so large that experts debate whether Internet access is, or should be, a human right.

The cyberspace-human rights relationship extends beyond the human rights regime because cyberspace creates human rights issues in other policy areas. This chapter considers four such areas—Internet governance, cybersecurity, trade in cyber technologies and services and the regulation of social media—in order to identify how human rights arise in cyber contexts across international politics (Part 5). In these areas, controversies have proliferated without resolution, raising questions about the effectiveness of human rights law in cyberspace.

The chapter concludes by assessing the trajectory of the cyberspace-human rights relationship from the optimism of the late 1990s into a darker, more uncertain future. An important trend is that human rights controversies multiplied as Internet access and use increased. Developments over the past decade, including Edward Snowden's revelations and the intensifying geopolitical rivalry between the US and China, have altered this relationship, especially concerning US power, influence and policy in cyberspace. Rather than becoming an exceptional phenomenon in human rights terms, cyberspace increasingly appears subordinate to the harsh international politics that adversely affected human rights in the past. This trajectory means the transformative human rights potential once associated with cyberspace has faded, and obstacles for reconstituting the cyberspace-human rights relationship on a new, constructive foundation are spreading.

2. INTERNET TECHNOLOGY, CYBERSPACE AND HUMAN RIGHTS

(a) Internet Technology and International Politics

In theory, human rights function independent of any technology. In practice, technologies affect whether and how individuals enjoy human rights. For example, under the principle of progressive realization, a State's obligations concerning economic, social and cultural rights expand as a country's economy develops—a process technology often drives. Innovations in communication technologies have also increased space for civil and political rights, such as the freedoms of expression and association.

In the evolution of communication technologies, telegraphy, telephony and radio emerged before the human rights movement began after World War II. The period associated with this movement witnessed the development of other communication technologies, including television, satellites and the Internet. Of these, the Internet is the most consequential for human rights. Although important, the telegraph, telephone and television—even enhanced by satellites—never generated a concept of 'telespace' as the Internet produced 'cyberspace'—an idea imbued with human rights significance from the start.[1]

The reasons for this difference are technological and political. Although the telegraph, telephone and television expanded cross-border communications, these technologies remained anchored geographically in ways that precluded conceptualizing them as creating a different realm of human interaction.[2] Politically, radio and tele-technologies emerged into multi-polar or bi-polar international systems characterized by great power competition that constricted how the technologies functioned within and among countries.

The Internet's emergence involves a different story. The technologies making up the Internet create a communication platform based on networks of interconnected computers sharing digital information through 'packet switching'. Rather than moving across a closed circuit (as a traditional telephone call did), data is broken into digital packets, transmitted over different routes in the networks, and reassembled at the destination. With standardized protocols, this approach is robust, achieves scale geographically, accommodates growing numbers of users and supports many applications.[3] The development of the World Wide Web improved Internet accessibility and expanded its use.

One way to sense how the Internet differs is to appreciate how it supports communications previously undertaken through older technologies. People now listen to the radio, watch television and make person-to-person voice and video calls over the Internet. It is the most multi-functional communication technology ever invented. The nature, interoperability and scalability of the component technologies mean the Internet can link millions of people around the world, accessibility and connectivity no previous technology achieved. The Internet is a technology of versatile capabilities and mass participation.

---

[1] For an historical comparison between the telegraph's emergence in the nineteenth century and the Internet, see Tom Standage, *The Victorian Internet* (Bloomsbury 2014).

[2] Wolfgang Kleinwächter, 'The history of internet governance' in Christian Möller and Arnaud Amouroux (eds), *Governing the Internet: Freedom and Regulation in the OSCE* (OSCE 2007) 41.

[3] David G Post, *In Search of Jefferson's Moose: Notes on the State of Cyberspace* (OUP 2009).

Although it has Cold War origins, the Internet did not become a phenomenon until the 1990s, the first decade of the post-Cold War world. US power, interests and ideas, along with the absence of great power competition, characterized this period. This international environment was unlike the political contexts that affected previous communication innovations. In addition, US dominance facilitated the rise of the Internet—an American invention—to global prominence. The Internet had political space in the post-Cold War period to take root and expand, and the Internet's technologies did not create technical barriers to exploiting that space.

The end of the Cold War also benefited human rights. The ideologically divisive, zero-sum game that the bipolar system inflicted on human rights efforts disappeared. The Vienna Conference on Human Rights in 1993—the first major post-Cold War human rights meeting—recognized the 'major changes taking place on the international scene' and embodied the energy the Cold War's end brought to human rights.[4]

(b) Cyberspace's Connection with Human Rights

These technological and political developments shaped thinking about 'cyberspace'—a new realm of communications and connectivity. Perspectives on cyberspace proliferated, highlighting the Internet's conceptual fertility. In one early, iconic view, the Declaration of the Independence of Cyberspace in 1996 framed cyberspace as a virtual world operating without government interference through a social contract created and implemented by individuals.[5] Others saw cyberspace as a new capability for promoting liberal political objectives—international peace achieved through economic interdependence among countries, democracy within countries and the individual's enjoyment of civil and political rights.

These perspectives envisioned cyberspace as a unique realm of human interaction favourable to global enjoyment of human rights. The capabilities of Internet technologies, the political space US dominance produced and re-energized interest in human rights converged to embed human rights in thinking about cyberspace. Borrowing from Waltz's levels of analysis,[6] this convergence framed cyberspace in 'first image' (the individual) and 'second image' (the State) terms by focusing on: (1) the individual's empowered and expanded communication opportunities; and (2) whether governments are democratic and protect human rights and, if not, how to use cyberspace to challenge and change non-democratic governments.

These perceptions worried authoritarian States, which, in response, opposed US power in cyberspace and emphasized the principles of sovereignty and non-intervention. This pushback appeared in forums discussing Internet governance and military power. In the early 2000s, China argued that Internet governance should be intergovernmental and subject to international law negotiated among States.[7] With US backing, Internet governance instead consisted of multi-stakeholder processes that produced non-legal outcomes achieved without governments negotiating as equals under international law. Authoritarian governments had problems

---

[4] World Conference on Human Rights, Vienna Declaration and Programme of Action, 25 June 1993.

[5] John P Barlow, 'A declaration of the independence of cyberspace,' *Electronic Frontier Foundation* (8 February 1996) https://projects.eff.org/~barlow/Declaration-Final.html accessed 28 August 2020.

[6] Kenneth N Waltz, *Man, the State and War: A Theoretical Analysis* (Columbia UP 1959).

[7] Kleinwächter (n 2) 55.

with this approach because it reflected US power and advanced interventionist policies that threatened their sovereignty.

Similarly, Russia highlighted the Internet's military potential and proposed measures to address a potential cyber arms race.[8] Although framed neutrally, these measures targeted the perceived US advantage in military cyber power. The US rejected these efforts because they cast suspicions on US cyber interests, behaviour and power.

The emphasis on sovereignty, non-intervention and the dangers of US cyber power attempted to shift thinking about cyberspace towards 'third image' (international system) considerations and away from democracy and human rights. This perspective subjected cyberspace to a traditional understanding of international order at odds with visions of cyberspace seeking progress on individual rights and the spread of democratic governance. The pushback turned Internet governance into a battleground between the 'Internet freedom' and 'Internet sovereignty' positions over the place of human rights in cyberspace (see Part 5).

3. CYBERSPACE, HUMAN RIGHTS AND GENERAL PRINCIPLES OF INTERNATIONAL LAW

(a) Challenges to General Principles of International Law

The emergence of human rights challenged general principles of international law developed before such rights appeared. By according rights to individuals in international law, States created friction for the principles on sovereignty, non-intervention, jurisdiction and State responsibility. For example, international human rights law stimulated disagreements over the extent to which a State's human rights obligations: (1) limited its sovereignty over its territory; (2) permitted other States to interfere in its domestic affairs; and (3) allowed it to regulate persons and activities outside its territory. The relationship of human rights to non-State actors, particularly multinational corporations, generated controversies about government responsibility to protect rights from private-sector behaviour and whether international law imposes human rights obligations on corporations.

The emergence of cyberspace challenged the same principles, and cyberspace controversies concerning these principles often involve human rights. The Internet sovereignty perspective emphasized the principles of sovereignty and non-intervention against foreign, cyber-facilitated support for civil and political rights and domestic political change. Arguments about how States exercise sovereignty and jurisdiction over online activities arose from incidents involving different conceptions of freedom of expression.[9] The difficulties encountered with attributing cyber actions to specific actors—as required under principles of State responsibility—have triggered concerns that governments exploit this problem and violate human rights (e.g., conducting surveillance against political opponents through proxies). How to protect rights, such as privacy, in corporate cyber activities has sparked disagreement. Whether Internet service providers (ISPs) and cyber technology companies have human rights obligations has replayed debates about the human rights duties of corporations.

---

[8] Tom Gjelten, 'Shadow wars: Debating cyber "disarmament"' (2010) *World Affairs* 33.

[9] Post (n 3) 164, discussing the French case against Yahoo! concerning Nazi memorabilia on an auction website.

(b) Between Universalism and Anarchy

Behind these challenges to general principles of international law is the convergence of a conceptual universalism in human rights thinking, and a technical universalism facilitated by Internet technologies. The idea of universal human rights predates cyberspace and is at the heart of the 'human rights v sovereignty' problem. However, in ways previous technologies did not achieve, the Internet makes communications borderless and fosters the idea that cyberspace is a new realm of human interaction. By contrast, general principles of international law reflect ideas grounded in the management of anarchy—the fragmentation of territorial control and political authority in the international system. Put differently, neither human rights (as a set of ideas) nor cyberspace (as a network of technologies) is Westphalian, and certainly not when combined. When human rights and cyberspace converge, pressure on Westphalian principles increases. Cyberspace takes on political significance through human rights that cyber technologies do not intrinsically have. Likewise, human rights take on a technological imperative, captured in the debate whether Internet access is a distinct human right.

These challenges to general principles of international law do not demonstrate that the challenges overwhelm the principles. The human rights movement encounters headwinds from frequent appeals to sovereignty and non-intervention. For example, the effort to re-calibrate human rights and sovereignty through the principle of the responsibility to protect proved controversial. In cyberspace, this chapter explores how authoritarian States have increased Internet access while strengthening their control and manipulation of online activities. Thus, cyberspace—even informed by human rights—has not killed sovereignty. Understanding how the cyberspace-human rights relationship affects international law also requires analysing specific areas of the law, a task the chapter addresses next.

4. CYBERSPACE AND THE HUMAN RIGHTS REGIME

In international relations, 'human rights' is more than an idea. It constitutes a regime—a set of problems, players, principles and processes that shape how individual rights are protected. This regime developed before the Internet and cyberspace emerged. As a result, this regime informs how cyberspace relates to rights in international law (Sections 4(a)–4(b)). Cyberspace has become important for protecting human rights and a focus for the regime's actors, institutions, processes and procedures. The manner in which the human rights regime applies to cyberspace informs the debate whether Internet access is, or should be, a new human right (Section 4(c)).

(a) Civil and Political Rights

International law recognizes civil and political rights connected with communications—the rights to freedom of expression and privacy. These rights protect private and public communications from government interference and facilitate enjoyment of other rights, including the rights to: freedom of opinion; freedom of thought, conscience and religion; freedom of association; and take part in public affairs. Freedom of expression and privacy support economic, social and cultural rights, including the rights to education and to take part in cultural life.

As an accessible, multi-functional communication platform, the Internet creates opportunities for people to impart and receive information and associate with others. Increasing use of Internet communications has made privacy a central cyberspace issue. Growing individual and social dependence on online communication heightens the importance of civil and political rights in cyberspace. The emphasis that Internet freedom accords to civil and political rights demonstrates how much these rights feature in political and legal discourse about cyberspace.

(i) Freedom of expression

Equating civil and political rights with Internet freedom would be misleading. Uniformity on civil and political rights relevant to communications did not prevail, even among democracies, before cyberspace emerged. Differences on freedom of expression exist between the US, with its sweeping protections of free speech, and many European democracies, which ban expression (e.g., Holocaust denial) the US tolerates. Treaties protecting freedom of expression, such as the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR), recognize that States parties can restrict enjoyment of this right for a number of reasons, including protecting the reputations of others, national security, public order, public health and morals.[10]

Variance on the scope of freedom of expression, combined with more online communication, has produced concerns about censorship in cyberspace:

> [M]any countries censor Internet content—dictatorships and democracies alike—and the number of countries doing so is growing every year. This set of censorial regimes includes … repressive regimes like China, North Korea, and others … but also … liberal democracies like the U.K., other western democracies, Asian democracies like South Korea, as well as Canada and Australia.[11]

Identifying Internet censorship in democratic and authoritarian States does not mean that both kinds of States restrict freedom of expression equally or in the same ways. Rather, the comparison underscores that rules on freedom of expression operate in more complicated ways than the 'freedom v sovereignty' dichotomy captures. National differences on freedom of expression demonstrate that international law accords some deference to sovereignty—what the European Court of Human Rights (ECtHR) calls the 'margin of appreciation' in protecting civil and political rights. The explosion of online communication has not harmonized the scope of freedom of expression. In fact, the way the Internet potentially makes all forms of information more accessible heightens State interests in restricting the right to send or receive certain kinds of communications. National differences on freedom of expression also highlight how this right connects with the principles of sovereignty, non-intervention and jurisdiction.

The complexity of international law reveals not only diversity in how States regulate speech but also the importance of procedural protections when governments restrict expression. The

---

[10] International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171 (ICCPR) Art 19; and European Convention on Human Rights and Fundamental Freedoms, 4 November 1950, 213 UNTS 221 (ECHR) Art 10.

[11] Dawn C Nunziato, 'How (not) to censor: Procedural First Amendment values and internet censorship' (2011) *Georgetown JIL* 1124, 1126.

ICCPR permits restrictions that 'are provided by law and are necessary',[12] which means that restrictions must be:

- Based on laws that are transparent, accessible and predictable;
- Related to a legitimate purpose that justifies restricting expression;
- Necessary and the least restrictive means available to achieve the purpose identified;
- Applied by an independent body free of political, commercial or other influences;
- Applied in a non-discriminatory and non-arbitrary manner; and
- Supported by safeguards against abuse, including the ability to challenge restrictions and remedy abuses.[13]

Human rights bodies have less tolerance for deviation from these procedural requirements, in contrast to the deference they often show States on the reasons for restricting freedom of expression. The jurisprudence of the ECtHR demonstrates how seriously it applies these requirements.[14] For example, in *Yildirim v. Turkey*, the Turkish Government prosecuted the owner of a Google-based website for insulting the memory of Kemal Ataturk.[15] A Turkish court blocked access to Google websites during the case. The ECtHR did not strike down the order because insulting Ataturk's memory is an illegitimate basis for restricting freedom of expression. Rather, it did so because the Turkish court order blocked access to websites having nothing to do with Ataturk, meaning the order had a disproportionate impact on the right to receive information. The migration of communications to the Internet, and the divergence that States exhibit on substantive protections for speech, heightens the importance of the procedural requirements for freedom of expression in cyberspace.

The complexity of the human rights regime is not the problem with countries that censor Internet communication with few, if any, protections. In 2016, the UN Special Rapporteur on the Right to Freedom of Opinion and Expression documented increasing restrictions on freedom of expression 'as States exploit society's pervasive need to access the Internet':

> Individuals seeking to exercise their right to expression face all kinds of limitations. Rationales are often unsustainable. Some of the limitations involve assertions of a legitimate objective — typically national security or public order — without the barest demonstration of legality or necessity and proportionality. Other limitations are based on objectives that are not legitimate under international human rights law.[16]

In 2018, Freedom House argued that 'global internet freedom declined for the eighth consecutive year' largely because a growing 'cohort of countries is moving toward digital authoritar-

---

[12] ICCPR (n 10) Art 19.3.

[13] Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/17/27, 16 May 2011, para 24.

[14] For an overview of the ECtHR's jurisprudence on the Internet and freedom of expression, see European Court of Human Rights, 'Factsheet: Access to internet and freedom to receive and impart information and ideas' (June 2020) https://www.echr.coe.int/Documents/FS_Access_Internet_ENG.pdf accessed 28 August 2020.

[15] *Ahmet Yildirim v. Turkey* App no 3111/10 (ECHR, 18 December 2012).

[16] UNGA, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/71/373, 6 September 2016, para 55.

ianism by embracing the Chinese model of extensive censorship and automated surveillance systems'.[17] Tactics used in digital authoritarianism include:

- Using firewalls to block or filter Internet content;
- Removing content critical of the government and its policies or officials;
- Revoking Internet access to punish political opponents or activism;
- Manipulating online communications through propaganda and misinformation;
- Adopting new laws that restrict and regulate online activities;
- Conducting surveillance of citizens through, including through artificial intelligence and facial recognition technologies;
- Arresting individuals for posting content online; and
- Using violence, including torture in detention, against political opponents active online.[18]

The rise of digital authoritarianism happened as governments increased Internet access. The International Telecommunication Union (ITU) estimated that the percentage of the global population using the Internet increased from 29.1 per cent in 2010 to 53.6 per cent in 2019.[19] Africa provides an example of increased Internet use occurring as digital authoritarianism spread. From 2005 to 2019, Internet use in Africa increased from 19 million people to 294 million.[20] However, '[o]ver the past two decades, authoritarian governments in Africa, with … help and inspiration from Chinese and Russian information control models, have tightened their grip on their national cyberspace by imposing internet censorship'.[21] This correlation between the growth of Internet use and digital authoritarianism challenges notions prevalent in the Internet's early years that cyber technologies undermine or overcome government censorship.[22]

The success of authoritarian governments in increasing Internet access and control over cyberspace highlights how governments can exploit cyber technologies and ignore human rights protections in international law. For example, Russia has increased Internet access over the past decade[23] and is a State party to the ICCPR and the ECHR. However, Russia has been in the vanguard of digital authoritarianism by adopting measures that 'severely undermine the ability of people in Russia to exercise their human rights online, including freedom of expression and freedom of access to information'.[24]

---

[17] Freedom House, *Freedom on the Net 2018: The Rise of Digital Authoritarianism* (2018) 1.

[18] Ibid., 6–19.

[19] ITU, 'Percentage of individuals using the internet, 2005–2019' https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx accessed 28 August 2020.

[20] Ibid.

[21] Babatunde Okunoye, 'Technologies of freedom enabling democracy in Africa', *Net Politics* (11 August 2020) https://www.cfr.org/blog/technologies-freedom-enabling-democracy-africa accessed 28 August 2020.

[22] For a critique, see Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (Public Affairs 2011).

[23] World Bank, 'Individuals using the internet (% of population)—Russian Federation' https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=RU accessed 28 August 2020.

[24] Human Rights Watch, 'Russia: Growing internet isolation, control, censorship' 18 June 2020 https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship accessed 28 August 2020.

(ii) Privacy

The human rights regime also protects the right to privacy.[25] This right, too, predates the Internet, but increasing use of cyber technologies creates many privacy issues. As with freedom of expression, international law applies to privacy online. However, problems often arise because countries, even democracies, do not agree on what privacy means.

For example, the US and the EU have experienced difficulties caused by different legal standards for protecting privacy and personal data.[26] Under the US Constitution, an individual has no reasonable expectation of privacy for information shared with third parties, such as ISPs.[27] Instead, a patchwork of federal and State statutes protect privacy.[28] By contrast, the EU has more comprehensive protections for privacy and data.[29] Approaches to privacy and data protection vary even more between democratic and authoritarian States.

Looking at international law on privacy, the ICCPR provides:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.[30]

These principles create negative and positive duties. First, ICCPR States parties cannot restrict the right to privacy unless government interference relates to a legitimate purpose and complies with procedural requirements. Legitimate purposes centre on surveillance for criminal law enforcement, counter-intelligence and national security (e.g., counter-terrorism). The procedural requirements mandate that surveillance has a legal basis, is authorized (e.g., by court order), and is necessary, meaning interference with privacy must be proportionate to the objectives sought.

Second, the ICCPR requires States parties to protect personal data that government agencies collect, store, process and use and regulate third parties to ensure protection of personal data from unlawful access and use. The ICCPR also gives individuals the right to ascertain what government agencies or third parties have their data and to have data revised if incorrect or purged if held or used without legal authorization.

However, describing legal doctrine does not convey the reality of government practices on privacy. A long-standing problem with surveillance involves expansive government readings of the legitimate purposes, such as protecting national security or fighting terrorism.[31]

---

[25] ICCPR (n 10) Art 17.

[26] For example, the EU Court of Justice has invalidated two US-EU data transfer agreements as incompatible with EU privacy and data protection law. See *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14, 8 October 2015, striking down the Safe Harbor agreement; and *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, Case C-311/18, 18 July 2020, striking down the Privacy Shield agreement.

[27] *Smith v. Maryland* 442 US 735 (1979).

[28] Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy* (Council on Foreign Relations Report), 30 January 2018 https://www.cfr.org/report/reforming-us-approach-data-protection accessed 28 August 2020.

[29] See Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of data (General Data Protection Regulation) [2016] OJ L119/1.

[30] ICCPR (n 10) Art 17.

[31] See, e.g., Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc A/

Authoritarian governments often interpret these purposes broadly and the procedural requirements narrowly (if they recognize them at all) in order to justify pervasive surveillance against persons considered actual or possible political opponents. Democracies have encountered criticism that surveillance activities for legitimate purposes, such as counter-terrorism, have questionable legal authority and disproportionately interfere with privacy.[32] Privacy advocates also lament inadequate protections for personal information stored, processed or used by governments or private-sector entities. Digital authoritarianism includes the pursuit of 'data sovereignty' over digital information—the imposition of 'rules and barriers in the name of national sovereignty, allowing officials to control and inspect such information at will'.[33] Differences between the US and the EU on legal requirements for private-sector handling of personal data has created privacy tensions over transatlantic data transfers, including the impact of EU data protection law on US corporations.[34] As with freedom of expression, such differences among countries on the substantive and procedural aspects of privacy reflect fragmentation and reinforce, in practice, the principles of sovereignty, non-intervention and jurisdiction.[35]

Online communication creates, however, additional problems for privacy and personal data protection. Privacy contributes to human dignity by protecting individual autonomy from government interference and private efforts to profit from personal information. Protecting autonomy becomes more difficult when individuals generate and share enormous amounts of information online. The proliferation of Internet-facilitated technologies, their increasing use and deepening dependence on them exacerbate this difficulty. Such massive production of digital data creates expanding opportunities for large-scale public and private storage, processing, analysis, utilization and surveillance of such data. These opportunities stimulate powerful commercial, law enforcement, national security and political incentives to access and 'mine' digital data, which puts constant strain on privacy rules. Further, the continued growth of cyber crime and cyber espionage indicates that protecting Internet-linked streams and reservoirs of digital data from unauthorized access and exploitation—as the right to privacy mandates—has proved difficult and controversial. These problems form part of debates about the future of privacy in the digital age.[36]

HRC/40/52, 1 March 2019, 11, criticizing 'the global emergence of overly broad and vague definitions of terrorism'. On cyber terrorism see Saul and Heath (Ch 10 of this Handbook).

[32] As discussed in Section 5(b) below, Snowden's disclosures in 2013–14 about electronic surveillance activities of the US and the UK sparked privacy controversies in and among democracies.

[33] Freedom House (n 17) 15.

[34] See, e.g., Adam Satariano, 'Google is fined $57 million under Europe's data privacy law', *NY Times* (21 January 2019) https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html accessed 28 August 2020.

[35] See Special Rapporteur on the Right to Privacy, Working Draft Legal Instrument on Government-led Surveillance and Privacy (Version 0.7), 28 February 2018, 3, proposing 'a new legal instrument … in the area of government-led or organized surveillance that could form the basis of a new global consensus among states' https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf accessed 28 August 2020.

[36] See Human Rights Council, The Right to Privacy in the Digital Age: Report of the UN High Commissioner for Human Rights, UN Doc A/HRC/39/29, 3 August 2018.

(b) Economic, Social and Cultural Rights

The human rights regime includes economic, social and cultural (ESC) rights, and the leading multilateral treaty is the International Covenant on Economic, Social and Cultural Rights (ICESCR).[37] An ICESCR State party accepts general obligations, including the principle of progressive realization, or the duty to 'take steps … to the maximum of its available resources' to achieve progressively full realization of the rights in the treaty.[38] ESC rights include the rights to: work; just and favourable working conditions; social security; an adequate standard of living; the highest attainable standard of health; education; partake in cultural life; and enjoy the benefits of scientific progress.[39]

(i) International law on ESC rights

International law on ESC rights creates three distinct obligations—the duties to respect, protect and fulfil. The duty to respect requires the State to refrain from restricting enjoyment of ESC rights. For example, under the right to health, the duty to respect prevents a government from denying or limiting access to health services.[40] The duty to protect obligates the State to ensure that third parties, such as corporations, do not threaten an individual's access to resources or services necessary for achieving ESC rights. In the health context, this duty calls for preventing private-sector entities from disseminating false or misleading health information.[41] The duty to fulfil mandates that the State must provide goods, resources or services critical to the enjoyment of ESC rights to persons unable to access or afford them. This obligation means the State has to provide health services to people without access to such services (e.g., rural communities) or who cannot pay for them (e.g., those in poverty).[42]

These duties involve immediate and unconditional obligations, such as ensuring government actions are not discriminatory, and requirements that give States a margin of discretion in how they realize ESC rights, such as in priority settings when government resources are limited. This discretion does not apply to 'minimum core obligations' that require the State to guarantee 'minimum essential levels of each right,' no matter the State's level of economic development and financial resources.[43] State actions that limit enjoyment of ESC rights are only permissible if they:

- Are based on clear, accessible laws that are not discriminatory, arbitrary or unreasonable and provide remedies for illegal or abusive actions;
- Promote the population's general welfare;

---

[37] International Covenant on Economic, Social and Cultural Rights, 16 December 1966, 993 UNTS 3 (ICESCR).

[38] Ibid., Art 2.1.

[39] Ibid., Arts 6–15.

[40] Committee on Economic, Social and Cultural Rights, General Comment No 14: The Right to the Highest Attainable Standard of Health, UN Doc E/C.12/2000/4, 11 August 2000, para 34.

[41] Ibid., para 35.

[42] Ibid., paras 36–37.

[43] Committee on Economic, Social and Cultural Rights, General Comment No 3 on the Nature of State Parties Obligations (art 2, para 1), Report of the Fifth Session, Supp No 3, Annex III, para 10, UN Doc E/1991/23, 14 December 1990.

- Do not impair the functioning of a democratic society (defined as a society that recognizes and respects human rights); and
- Do not jeopardize the essence of the rights being limited.[44]

This description of ICESCR principles does not communicate the controversies that international law on ESC rights has experienced. Despite the right to health being in the Constitution of the World Health Organization (1946), the Universal Declaration of Human Rights (UDHR, 1948) and the ICESCR (1966), a 1999 study argued that this right suffered from a 'lack of conceptual clarity and … weak international and national implementation'.[45] The principle of progressive realization has been at the heart of many ESC rights controversies. The idea that enjoyment of ESC rights depends on the level of a country's economic development makes these rights seem, to many, like political aspirations rather than legal rights. Further, critics have argued that, without protections for civil and political rights, ESC rights are not secure. For example, without freedom of expression, the ability to change government policies to advance ESC rights is undermined. In addition, under the margin of discretion, States can use the principles of sovereignty and non-intervention to deflect outside concerns about their compliance with ESC rights.

(ii) ESC rights and cyberspace

Human rights advocates frequently link the Internet with enjoyment of ESC rights. Growing dependence on cyberspace gives online information increasing prominence in progressive realization of ESC rights. Using the right to health again as an example, the duty to respect means a government cannot limit or deny people access to valid online health information and services. The duty to protect obligates governments to prevent fraud by third parties involving health information, goods and services (e.g., online sales of falsified medicines). The duty to fulfil requires a government to enable or expand Internet access to information and services that health care providers and individuals can use to improve health.

The work of the Committee on Economic, Social and Cultural Rights (ESCR Committee) illustrates that Internet access arises in evaluating State party performance under the ICESCR. In its 2019 review of the implementation report from Nicaragua, the ESCR Committee asked what steps the Nicaraguan Government had taken under the right to partake in cultural life 'to ensure affordable access to the Internet for disadvantaged and marginalized persons and groups, including in rural areas'.[46] However, cyberspace's relationship with ESC rights should be kept in perspective. Internet access is not a minimum core obligation because it is not critical to human subsistence. In terms of progressive realization, many States parties face problems implementing ESC rights for which an individual's Internet access is not a priority, including obligations to provide people with adequate water, sanitation, food, housing and essential medicines. Not every ESCR Committee review of State party reports mentions the Internet, and the Committee's guidelines on State party reports mention the Internet only once, in connection with enhancing 'access to the cultural heritage of mankind, including through

---

[44] ICESCR (n 37) Art 4; Limburg Principles on the Implementation of the International Covenant on Economic, Social and Cultural Rights http://www.escr-net.org/docs/i/425445 accessed 28 August 2020.

[45] Brigit C A Toebes, *The Right to Health as a Human Right in International Law* (Hart 1999) 85.

[46] Committee on Economic, Social and Cultural Rights, List of Issues in relation to the Fifth Periodic Report of Nicaragua, UN Doc E/C.12/NIC/Q/5, 13 November 2019, 5.

new information technologies such as the Internet'.[47] Only two of the ESCR Committee's 15 general comments interpreting ESC rights issued in the Internet era mention Internet access or use.[48] Nor does it appear that Internet access or use features in cases brought under the ICESCR's Optional Protocol, which allows individuals to submit claims of ICESCR violations to the ESCR Committee.[49]

(iii) The 'digital divide,' ESC rights and the right to development

Enjoyment of ESC rights connects to the 'digital divide'—the gap between developed and developing countries in access to the Internet and other information communication technologies (ICTs). It also encompasses the ICT gap within countries between, for example, urban and rural areas. Reducing the digital divide is part of development strategies, including how increasing access to ICTs and the Internet can contribute to the UN's Sustainable Development Goals.[50]

The digital divide also highlights the Internet's role in the 'right to development'. The UN General Assembly declared in 1986 that everyone and all peoples have an inalienable right to 'participate in, contribute to, and enjoy economic, social, cultural and political development'.[51] According to the UN High Commissioner for Human Rights:

> Since the adoption of that landmark document, a debate has been raging … On one side, proponents of the right to development assert its relevance (or even primacy) and, on the other, sceptics (and rejectionists) relegate this right to secondary importance, or even deny its very existence. Unfortunately, … that debate has done little to free the right to development from the conceptual mud and political quicksand in which it has been mired all these years.[52]

This controversy has not prevented human rights advocates from making cyberspace important to the right to development. The Human Rights Council recognized 'the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms'.[53] The World Federation of University Women emphasized that Internet access

---

[47] Committee on Economic, Social and Cultural Rights, Guidelines on Treaty-Specific Documents to be Submitted by States Parties under Articles 16 and 17 of the International Covenant on Economic, Social, and Cultural Rights, UN Doc E/C.12/2008/2, 24 March 2009, para 67.

[48] Committee on Economic, Social and Cultural Rights, General Comment No 21 on the Right of Everyone to Partake in Cultural Life, UN Doc E/C.12/GC/21, 21 December 2009, para 32; and Committee on Economic, Social and Cultural Rights, General Comment No 25 on Science and Economic, Social and Cultural Rights, UN Doc E/C.12/GC/25, 30 April 2020, paras 16 and 42.

[49] Optional Protocol to the International Covenant on Economic, Social and Cultural Rights, 10 December 2008, 2922 UNTS 29.

[50] Adopted in 2015, the Sustainable Development Goals include the target of increasing ICT access and striving to provide universal, affordable access to the Internet in least developed countries by 2020. UN, Sustainable Development Goals, Goal 9—Build Resilient Infrastructure, Promote Sustainable Industrialization and Foster Innovation, Target 9.C https://www.un.org/sustainabledevelopment/infrastructure-industrialization/ accessed 28 August 2020. See also ITU, *ICTs, LDCs and the SDGs: Achieving Universal and Affordable Internet in the Least Developed Countries* (ITU 2018).

[51] UNGA, Declaration on the Right to Development, UN Doc Res 41/128, 4 December 1986.

[52] Navi Pillay, UN High Commissioner for Human Rights, 'Development is a human right for all' http://www.ohchr.org/EN/ISSUES/DEVELOPMENT/Pages/DevelopmentIndex.aspx accessed 28 August 2020.

[53] Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, UN Doc A/HRC/20/L.13, 29 June 2012, 2.

was key to women's enjoyment of the right to development, which required attention to the gender implications of the digital divide.[54]

However, efforts by the UN Working Group on the Right to Development and the High-Level Task Force on the Implementation of the Right to Development indicate that the digital divide has not been the most prominent concern related to access to technologies. Working Group and Task Force reports demonstrate that other technology transfer issues, such as tension between intellectual property rights and access to essential medicines, have received more attention than Internet access and the digital divide. Technology transfer has long been a problem for development policy. However, Internet access does not resemble the technology transfer controversies that dominate policy discussions. Cyber technologies have spread globally and are not generally subject to the limitations that trigger technology transfer problems, such as export controls on 'dual use' technologies and protection of intellectual property rights.

(c) Internet Access as a New Human Right?

The Internet features so prominently across the human rights regime that people debate whether Internet access is, or should be, a human right. As the Special Rapporteur on the Right to Freedom of Opinion and Expression put it, 'the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress'.[55] Framing the Internet in this way is consistent with seeing technologies as means for protecting and promoting human rights. For example, health advocates consider access to technologies, such as vaccines, as important instruments in achieving the right to the highest attainable standard of health.

Many arguments associated with the 'Internet access is a human right' position reflect this instrumental approach. Former Secretary of State Hillary Clinton articulated a 'freedom to connect' to the Internet, but this freedom depends on other civil and political rights—namely, the freedoms of opinion, expression and assembly.[56] Similarly, Mark Zuckerberg, founder of Facebook, argued that Internet connectivity is a human right because such connectivity is a means for achieving political, economic and social objectives that the human rights regime already targets.[57] Vint Cerf, one of the Internet's creators, argued that 'Internet access is just a tool for obtaining something else more important'.[58] The UN Human Rights Council took this position in affirming that people have the same human rights online as they do offline.[59]

The idea of Internet access as a distinct right differs from the instrumental perspective by positing that access is, by itself, so central to individual life, autonomy or dignity that it

---

[54] Report of the Open-Ended Working Group on the Right to Development, UN Doc E/CN.4/2001/26, 20 March 2001, para 138.

[55] Special Rapporteur's Report (n 16) para 85.

[56] Hillary Clinton, 'Remarks on internet freedom,' 21 January 2010 https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm accessed 28 August 2020.

[57] Mark Zuckerberg, 'Is connectivity a human right?' https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-ash3/851575_228794233937224_51579300_n.pdf accessed 28 August 2020.

[58] Vint Cerf, 'Internet access is not a human right', *NY Times* (4 January 2012) http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html accessed 28 August 2020.

[59] Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, UN Doc A/HRC/RES/32/13. 18 July 2016, 3.

deserves protection as a fundamental right. For example, Merten Reglitz took issue with the Human Rights Council's position because Internet access 'is necessary for people to be able to lead minimally decent lives' which 'transforms our conception of the Internet from a technology to that of a basic right'.[60] This argument elevates Internet access to an equivalent status with human rights problems that pose grave threats to the world's marginalized populations, such as lack of clean water, food insecurity, inadequate health care, environmental degradation, poor education, and political or criminal violence.

5. INTERNATIONAL RELATIONS AND THE CYBERSPACE-HUMAN RIGHTS RELATIONSHIP

Cyberspace affects international relations beyond human rights, which calls for examining how State behaviour in other areas connects to the cyberspace-human rights relationship. This part looks at Internet governance, cybersecurity, trade in cyber technologies and the regulation of social media as contexts in which human rights issues have emerged. The ways in which human rights arise are controversial, reveal disagreements about human rights in the Internet age and raise questions about the prospects of the human rights regime in cyberspace's future.

(a) Internet Governance

This chapter previously mentioned the conflict between Internet freedom and Internet sovereignty concerning Internet governance. The international politics of Internet governance involve great power competition, disagreements about what problems Internet governance addresses, divergent views about non-State actor participation and friction over civil and political rights. Although the Internet governance controversy is broad, human rights are a prominent and divisive feature.

Internet freedom views cyberspace as a means for advancing civil and political rights, the spread of democracy, and multi-stakeholder governance—the collaboration of public, corporate and civil society stakeholders. Internet freedom is transformative—the Internet and cyberspace can help change domestic and international politics. By contrast, Internet sovereignty embeds cyberspace in an international order that functions through inter-State governance, the balance of power and the principles of sovereignty and non-intervention. Internet sovereignty is conservative—States must discipline the Internet through traditional mechanisms for maintaining order among and within sovereign States.

These conflicting perspectives have clashed in negotiations on Internet governance. For example, the ITU convened the World Conference on International Telecommunications (WCIT) in 2012 to revise the International Telecommunication Regulations (ITRs). The negotiations failed because of the fault line between Internet freedom and Internet sovereignty. Countries associated with Internet freedom, especially the US and European democracies, rejected the revisions because they contained provisions that threatened civil and political rights, such as freedom of expression. China, Russia and other authoritarian countries linked with Internet sovereignty supported the revisions because they reflected their desire to expand

[60] Merten Reglitz, 'The human right to free internet access' (2020) 37 *Journal of Applied Philosophy* 314 https://onlinelibrary.wiley.com/doi/abs/10.1111/japp.12395 accessed 28 August 2020.

the political scope of Internet governance and strengthen inter-governmental control of such governance.

This stalemate indicated that Internet sovereignty had grown in influence and impact. China, Russia and supportive countries prevailed in getting Internet governance on the ITU's agenda, succeeded in negotiating new ITR provisions they wanted and held firm against US and European opposition. The WCIT represented a culmination of authoritarian efforts, dating back to the turn of the century, to make Internet governance reflect their interests. Since the WCIT, efforts based on Internet sovereignty continued apace,[61] contributing to a sense that Internet freedom faces a crisis.[62] From a human rights perspective, these developments are unwelcome because the States leading the charge on Internet sovereignty are behind the global spread of digital authoritarianism.

(b) Cybersecurity

As other chapters in this volume analyse, cybersecurity has become a significant concern, including from a human rights perspective. Cybersecurity threats from criminals, terrorists, intelligence agencies and militaries have provoked governments to respond in ways that human rights advocates believe infringe civil and political rights.[63] The disclosures Edward Snowden made in 2013–14 about US cyber surveillance and cyber espionage activities sparked controversies about the threats these activities posed to civil and political rights.[64] The proliferation of cybersecurity problems suggests that cyberspace is insecure and dangerous in ways that undermine using the Internet to advance human rights.

Over the past two decades, concerns about cybersecurity threats have relentlessly increased. Cyber attacks by criminals, fears about cyber terrorism, cyber espionage by foreign governments and development of military cyber weapons by rival countries have forced States to devote more attention to cybersecurity. Strategies for responding to cybersecurity vulnerabilities have raised human rights questions. For example, improving defences against malicious cyber operations requires 'situational awareness', achieved by expanded surveillance of cyberspace and more information sharing between non-governmental actors and government agencies. Those focused on protecting freedom of expression and privacy often oppose these strategies because they tend to increase government power without adequate safeguards for these rights.[65]

---

[61] See, e.g., Chinese and Russian support for, and US opposition to, the General Assembly's establishment of an (1) Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (UN Doc A/RES/73/27, 11 December 2018); and (2) Open-Ended Ad Hoc Committee of Experts to elaborate an international convention on countering the use of ICTs for criminal purposes (UN Doc A/RES/74/247, 27 December 2019).

[62] Jack Goldsmith, 'The failure of internet freedom' (Knight First Amendment Institute, 13 June 2018) https://knightcolumbia.org/content/failure-internet-freedom accessed 28 August 2020.

[63] On cyber operations and international human rights law, see Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) 179–208.

[64] For perspectives on, and primary documents from, Snowden's disclosures, see David P Fidler (ed), *The Snowden Reader* (Indiana UP 2015). On cyber espionage and international law see Buchan and Navarrete (Ch 11 of this Handbook).

[65] Controversies about privacy arose in the US during adoption of the Cybersecurity Information Sharing Act (CISA) of 2015, leading to the development of privacy and civil liberties guidelines.

A different, but related, worry involves authoritarian governments using cybersecurity threats as an excuse for expanding surveillance in order to repress political opposition. China's control and censorship of Internet activities demonstrate that, for the Communist Party, cybersecurity means protecting against any use of cyberspace that challenges its authority and power. China's cybersecurity and data protection laws 'risk compromising data security for the sake of increasing government accessibility to private information'.[66] The treaty on information security concluded by the Shanghai Cooperation Organization, the members of which are authoritarian States (including China and Russia), defines terms—such as 'information security', 'information crime' and 'information terrorism'—in ways that demonstrate no interest in protecting freedom of expression and privacy in cyberspace.[67]

Snowden's disclosures about US cyber surveillance and espionage damaged the Internet freedom agenda because they exposed the US Government's willingness to conduct cyber surveillance on a global scale against friend and foe alike. Michael Hayden, former director of the National Security Agency (NSA) and Central Intelligence Agency, admitted that the US could be accused of militarizing cyberspace after what Snowden revealed[68]—an accusation corrosive to US claims of leadership on Internet freedom.

Snowden's leaks also sparked privacy debates in the US and globally. Within the US, Snowden exposed NSA programs that collected domestic telephony metadata in bulk and massive amounts of communications between US persons and foreign intelligence targets located outside the US. Privacy advocates challenged these programs. In response, Congress ended the NSA's bulk collection of domestic telephony metadata and changed how the NSA collects communications between US persons and foreign intelligence targets outside the US.[69]

Internationally, Snowden's revelations about US cyber espionage against allied and friendly countries produced a backlash against the US. In response to NSA cyber spying, Germany and Brazil introduced a draft resolution at the UN that applied the right to privacy to surveillance conducted by States outside their territories.[70] This effort recalled earlier controversies about whether human rights obligations apply when a country acts outside its territory.[71] But, the draft resolution contained a more radical proposition—that a State's espionage against foreign targets located outside its territory are subject to the right to privacy in international law. Following its long-held position that ICCPR obligations do not extend outside its territory, the US opposed the extraterritorial application of the right to privacy. The revised resolution

---

See Department of Homeland Security and Department of Justice, *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* (15 June 2018).

[66] Lauren Maranto, 'Who benefits from China's cybersecurity laws?', *New Perspectives on Asia* (25 June 2020) https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws accessed 28 August 2020.

[67] Shanghai Cooperation Organization, Agreement on Cooperation in the Field of International Information Security, December 2008.

[68] Andrea Peterson, 'Former NSA and CIA Director says terrorists love using gmail' *Washington Post* (15 September 2013) https://www.washingtonpost.com/news/the-switch/wp/2013/09/15/former-nsa-and-cia-director-says-terrorists-love-using-gmail/ accessed 28 August 2020.

[69] USA FREEDOM Act, Public Law 114-23 (2 June 2015), ending bulk collection of domestic telephony metadata; and FISA Amendments Reauthorization Act, Public Law 115-118 (19 January 2018), making changes to surveillance of communications of foreign intelligence targets outside the US.

[70] UNGA, The Right to Privacy in the Digital Age, UN Doc A/C.3/68/L.45, 1 November 2013.

[71] See, e.g., Marko Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (OUP 2011).

contained compromise language that permitted both sides to claim victory.[72] The General Assembly approved this resolution without a vote, another indication of the disagreements it created.[73]

The UN followed this resolution with activities focused on the right to privacy. The UN High Commissioner for Human Rights analysed the right to privacy in the digital age, concluding that the practice of many States 'revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy'.[74] The Human Rights Council appointed the first-ever Special Rapporteur on the Right to Privacy with the mandate, among other things, to address the challenges that the digital age presents to protecting privacy.[75]

In response to concerns other countries raised, President Obama instructed the US intelligence community to protect the privacy interests of all persons, including non-US persons located outside the US.[76] Specifically, US intelligence activities must 'include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual … or where that individual resides'.[77] This directive remains in force. Although framed as protecting privacy 'interests' rather than 'rights', the directive is, Benjamin Wittes argued, 'an amazing statement' because the US declared 'that it respects the privacy of non-citizens abroad and takes that into account when it conducts espionage'.[78]

However, responses to Snowden's disclosures at the UN and in the US do not mean that State practice reflects widespread acceptance that privacy and other human rights apply extraterritorially to government intelligence activities. The countries to which Snowden fled—China and then Russia—practice digital authoritarianism and export this approach to other nations, hardly evidence that these countries believe international human rights law regulates their intelligence activities. In particular, human rights advocates have warned that China's surveillance inside other countries contributes to the problem 'that Chinese censorship is becoming a global threat' for individuals, corporations and universities outside China.[79]

---

[72] UNGA, The Right to Privacy in the Digital Age, UN Doc A/C.3/68/L.45/Rev. 1, 20 November 2013.

[73] UNGA, The Right to Privacy in the Digital Age, UN Doc A/RES/68/167, 18 December 2013.

[74] Human Rights Council, The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights, UN Doc A/HRC/27/37, 30 June 2014, para 47.

[75] Human Rights Council, The Right to Privacy in the Digital Age, UN Doc A/HRC/RES/28/16, 1 April 2015, para 4.

[76] Presidential Policy Directive/PPD-28—Signals Intelligence Activities, 17 January 2014, § 4.

[77] Ibid.

[78] Benjamin Wittes, 'The president's speech and PPD-28: A guide for the perplexed' (20 January 2014) *Lawfare*, https://www.lawfareblog.com/presidents-speech-and-ppd-28-guide-perplexed accessed 28 August 2020. But see Brennan Center for Justice et al, *National Security Surveillance and Human Rights in a Digital Age—United States: A Joint Submission to the United Nations Human Rights Council* (April-May 2015) 11, criticizing PPD-28's provisions on the privacy of non-US persons.

[79] Kenneth Roth, 'China's global threat to human rights' in Human Rights Watch, *World Report 2020* (Human Rights Watch 2020) 1, 15. See also UN Office of the High Commissioner for Human Rights, 'UN experts call for decisive measures to protect fundamental freedoms in China', 26 June 2020 https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26006&LangID=E, warning about China's 'interferences with the right to privacy' and 'cybersecurity laws that authorise censorship'.

Snowden also disclosed information about US cyber espionage against adversaries, including China, Russia and Iran. The disclosures gave rival States insights into US cyber power and encouraged them to strengthen their own intelligence and military cyber capabilities. The leaks vindicated rival States' claims that US cyber operations targeted them, provided ammunition for accusing the US of hypocrisy on human rights in cyberspace and deepened their commitment to Internet sovereignty. Such *realpolitik* reactions to Snowden's revelations undermined prospects for protecting civil and political rights in cyberspace and using the Internet to achieve progressive realization of ESC rights.

The Snowden incident heightened human rights interest in using encryption to communicate online in an increasingly insecure cyberspace. This development agitated concerns that encryption would undermine law enforcement and national security efforts to thwart online crime, terrorism and foreign espionage. Government worries about the 'going dark' problem provoked a controversy that stimulated debate about human rights and encryption. The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression argued that '[e]ncryption and anonymity provide … a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks'.[80] In addition, encryption creates security online that facilitates 'the exercise of other rights, including economic rights, privacy, due process, freedom of assembly and association, and the right to life and bodily integrity'.[81] Thus, the Special Rapporteur concluded, 'restrictions on encryption and anonymity must be strictly limited to principles of legality, necessity, proportionality and legitimacy in objective'.[82]

Encryption debates have been complicated because governments in democratic and authoritarian countries see both the benefits and threats that encrypted communications and data create.[83] In line with Internet sovereignty, authoritarian States have moved more aggressively to counter the threat that encryption poses to the control and censorship of online activities. In democracies, government interest in addressing law enforcement and national security problems associated with encryption has not so far succeeded in quelling controversy. For example, problems have dogged the Australian law adopted in 2018, with Australia's Independent National Security Legislation Monitor calling for it to be comprehensively revised.[84] In the US, successive presidential administrations have highlighted the 'going dark' problem without, to date, achieving the legislation believed necessary to mitigate the law enforcement and national security challenges that encryption produces.

---

[80] Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/29/32, 22 May 2015, para 16.

[81] Ibid., para 56.

[82] Ibid.

[83] On the US encryption debate, see Berkman Center for Internet and Society, *Don't Panic: Making Progress on the 'Going Dark' Debate* (Harvard University, 1 February 2016). For China, see Lorand Laski and Adam Segal, *The Encryption Debate in China* (Carnegie Endowment for International Peace, 30 May 2019).

[84] Paul Karp, 'Australia's world-first anti-encryption law should be overhauled, independent monitor says', *The Guardian* (9 July 2020) https://www.theguardian.com/australia-news/2020/jul/09/australias-world-first-anti-encryption-law-should-be-overhauled-independent-monitor-says accessed 28 August 2020.

(c) Private Enterprise, Human Rights and Cyber Technologies

Human rights issues arise in connection with the private sector's development, use and sale of cyber technologies and services. As mentioned above, migration of information and communication online gives companies, especially ICT enterprises, access to massive amounts of data. Privacy advocates are concerned that laws in many countries, including the US, do not sufficiently protect privacy from corporate interests. Human rights groups have also criticized ICT companies for undermining freedom of expression by: (1) cooperating with the efforts of authoritarian governments to censor and control the Internet; and (2) selling cyber technologies to repressive regimes that use them against political opponents. As has happened in other contexts involving private-sector behaviour,[85] advocacy has sought to apply international human rights law to corporate activities in cyberspace.

These concerns and this strategy informed creation of the Global Network Initiative (GNI), a voluntary, multi-stakeholder effort focused on helping ICT companies advance freedom of expression and privacy through independent reviews of corporate member compliance with GNI's principles, which are informed by international human rights law.[86] For privacy, the EU's General Data Protection Regulation has been an important development because it compels companies, wherever located, that process data from nationals of EU members to comply with the regulation.[87] Countries participating in the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies agreed to restrict exports of 'dual use' ICT products, such as intrusion software and network surveillance systems, that governments could use to violate civil and political rights.[88] In response to concerns that the restrictions prevented the export of legitimate cybersecurity products and services, the Wassenaar Arrangement members revised the export controls.[89] However, such efforts to improve corporate commitment to freedom of expression and privacy have not deterred authoritarian countries, especially China, from exporting technologies for monitoring, controlling and censoring Internet activities.[90]

(d) Regulation of Social Media

As the second decade of this century began, the 'Arab Spring' protests in North Africa and the Middle East used US-based social media platforms to advance the democracy and human rights agendas associated with Internet freedom. Within a few years, democracies were reeling from terrorists and authoritarian governments using social media to threaten national security,

---

[85] See UN, *Guiding Principles on Business and Human Rights* (UN 2011).

[86] Global Network Initiative, *The GNI Principles at Work: Public Report on the Third Cycle of Independent Assessments of GNI Company Members 2018-2019* (GNI 2019).

[87] Freedom House (n 17) 18.

[88] Public Statement: 2013 Plenary Meeting of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, 4 December 2013.

[89] Garrett Hinck, 'Wassenaar export controls on surveillance tools: New exemptions for vulnerability research' (5 January 2018) *Lawfare*, https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research accessed 28 August 2020.

[90] Freedom House (n 17) 7–8, describing China's efforts to export its model of digital authoritarianism.

violate human rights and undermine democracy.[91] Worries also mounted within democracies that groups with extremist agendas, such as white supremacists, were exploiting social media to increase their malicious influence. These developments produced a crisis for social media and sparked controversies about the regulation of social media that implicated human rights.

Generally, authoritarian governments responded to the threat that social media presented by restricting or banning foreign platforms and subjecting domestic social media services to extensive surveillance, control and censorship. For example, China banned Facebook and censors Chinese social media platforms, such as Weibo. Authoritarian governments also use 'social media surveillance tools that employ artificial intelligence to identify perceived threats and silence undesirable expression'.[92] The application of digital authoritarianism to social media has produced 'a sharp global increase in the abuse of civil liberties and shrinking online space for civic activism'.[93] In addition, authoritarian governments exploit social media platforms by spreading propaganda and disinformation at home to maintain power and abroad to influence politics in foreign countries.[94]

By contrast, democracies, especially the US, have struggled to counter malign social media activity by terrorists, foreign governments, home-grown extremist groups and domestic political actors. Such confusion and hesitation flow from the commitment of democracies to freedom of expression, which limits government authority to engage in online censorship. As a result, political pressure has mounted on companies that operate social media platforms to regulate online content, a task these enterprises have proved reluctant or ill-equipped to undertake.[95] Social media in democracies remain essentially ungoverned, which invites illiberal actors to manipulate cyberspace in ways that jeopardize the promotion and protection of human rights and undermine Internet freedom. The situation is so dire that, according to Freedom House, 'the future of internet freedom rests on our ability to fix social media'.[96]

---

[91] On terrorist use of social media, see Alberto M Fernandez, *Here to Stay and Growing: Combating ISIS Propaganda Networks* (Brookings U.S.-Islamic World Forum Paper, October 2015). On authoritarian government use of social media to undermine democracy, see Robert S Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (Department of Justice, March 2019) 14–35, analyzing Russia's disinformation campaign on social media during the US election in 2016.

[92] Freedom House, *Freedom on the Net 2019: The Crisis of Social Media* (2019) 2.

[93] Ibid.

[94] Ibid., 1.

[95] For example, Mark Zuckerberg, founder of Facebook, rejected calls for Facebook to regulate online speech. Cecilia Kang and Mike Isaac, 'Defiant Zuckerberg says Facebook won't police political speech', *New York Times* (17 October 2019) https://www.nytimes.com/2019/10/17/business/zuckerberg-facebook-free-speech.html accessed 28 August 2020. Less than a year later, as political anger about disinformation on social media continued to increase, Zuckerberg acknowledged that Facebook has a responsibility to combat the abuse of its platform by bad actors. Betsy Woodruff Swan, 'Zuckerberg: Facebook has "more to do" on fighting disinformation', *Politico* (26 July 2020) https://www.politico.com/news/2020/07/28/zuckerberg-opening-statement-house-hearing-384824 accessed 28 August 2020.

[96] Freedom House (n 92) 2.

6. CONCLUSION

The complexity of the cyberspace-human rights relationship makes finding its critical features difficult, if not foolhardy. The relationship emerged at a unique historical moment when unprecedented political conditions facilitated innovative technologies of communication that promised to strengthen human rights. The many ways that the human rights regime applies to the Internet—and the human rights activism on cyberspace issues—constitute partial fulfilment of this promise. However, political, legal and technological developments have adversely affected the relationship in ways that burden the present and threaten the future.

Politically, the uni-polar moment of the post-Cold War period is over, replaced by intensifying geopolitical competition among the great powers and their incompatible interests on the Internet and human rights. Legally, all-too-familiar gaps between legal doctrine and State practice on human rights have appeared again in the cyberspace-human rights relationship. Technologically, authoritarian governments have managed to expand Internet access while increasing censorship and control over cyberspace. For its part, the US harnessed cyber technologies for commercial, intelligence and military purposes in ways that human rights advocates believe have damaged what cyberspace should mean for human rights.

The prowess of authoritarian governments in monitoring and manipulating online activities, the momentum of Internet sovereignty, and the struggles of democracies with social media converge to produce the most dangerous conditions that the relationship between cyberspace and human rights has yet faced. Although the Internet is the most consequential communication technology of the human rights era, it has not proven to be an exceptional technology in transforming the human rights project in domestic or international politics. Looking ahead, the primary human rights challenges in cyberspace involve grappling with age-old political problems, including the tenacity of sovereignty, the resiliency of authoritarianism, the complexities of democracies, the difficulty of balancing human rights and national security and the consequences of shifts in the distribution of power in the international system.

8. International criminal responsibility in cyberspace

Kai Ambos[1]

1. INTRODUCTION: SCOPE AND CONCEPTUAL CLARIFICATIONS

Given the methodology and purpose of a Research Handbook the primary objective of this chapter will be to give a reliable overview of the state of the art with regard to the topic. This is not an easy task given its great uncertainty, complexity and dynamics.[2] In any event, given the broad scope of both 'criminal responsibility' and 'cyberspace' we have, first of all, to determine more precisely the scope of the inquiry.

(a) Focus on Cyber Attacks

While 'cyberspace' may be broadly defined as a domain characterized by 'the use of electronics … and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures'[3] and thus 'cybercrime' encompasses a wide variety of criminal activity by means of or in the world wide web (from criminal economic

[1] I thank my doctoral student Luca Petersen for assistance in preparing the updated version of this chapter.

[2] This is admitted at the outset in the serious publications on the matter, see, e.g., David Turns, 'Cyber warfare and the notion of direct participation in hostilities' (2012) 17 *J of Conflict & Security L* 280, 282, stating that it is 'rather difficult to write authoritatively about international law and CW [cyber warfare]: one has a distinct feeling of the ink not yet being dry on the page'.

[3] US Department of Defense according to Herbert Lin, 'Cyber conflict and international humanitarian law' (2012) 94 *Intl Rev of the Red Cross* 515, 516; similarly, Michael N Schmitt, 'Classification of cyber conflict' (2012) 17 *J of Conflict & Security L* 245, 258. On the differences between conflict in cyberspace and physical space (i.e., traditional conflict) see Lin, ibid., 520.

activity to copyright violations and child pornography),[4] this chapter will only focus on cyber attacks.[5]

A cyber attack is the strongest form of a cyber operation which itself is an umbrella term referring to 'employment of cyber capabilities to achieve objectives in or through cyberspace'.[6] Other forms of cyber operations are cyber espionage[7] and cyber manipulation, the latter even a broader umbrella term.[8] Cyber attacks can be regarded as part of cyber warfare,[9]

---

[4] It is not easy to find a comprehensive definition of the term 'cybercrime'. It is often interchangeably used with the terms 'computer crime', 'computer-related crime', 'high-tech crime' and 'cybercrime'. The Cybercrime Convention of the Council of Europe of 23 November 2001 lists: illegal access; illegal interception; data interference; system interference; misuse of devices; computer-related forgery; computer-related fraud; offences related to child pornography; and to infringements of copyright and related rights (Arts 2–10). The AP of 28 January 2003 adds to this impressive list acts of a racist and xenophobic nature committed through computer systems. EU documents take a similarly broad approach covering any conduct that describes: 'a) the use of information and communication networks that are free from geographical constraints; and b) the circulation of intangible and volatile data', see European Commission, 'Fight against cybercrime' (12 September 2005) https://web.archive.org/web/20150406150834/http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193b_en.htm accessed 6 Oct. 2021. For a similar broad definition from an US perspective see Oona A Hathaway and others, 'The law of cyber-attack' (2012) 100 *California L Rev* 817, 833; David Weissbrodt, 'Cyber-conflict, cyber-crime, and cyber espionage' (2013) 22 *Minnesota of J Intl L* 345, 366–70.

[5] The previously used term 'computer network attack (CNA)' which has probably its roots in the *object-based-approach* seems meanwhile obsolete; *cf* Reese Nguyen, 'Navigating jus ad bellum in the age of cyber warfare' (2013) 101 *California L Rev* 1079, 1088. Given the variety of terms and definitions, often used similarly or even identically, terminological precision is required.

[6] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) [hereinafter 'Tallinn Manual 2.0'], 564. Critically on the Manual's methodological approach and the composition of the Expert group see Oliver Kessler and Wouter Werner, 'Expertise, uncertainty, and international law: A study on the Tallinn Manual on cyberwarfare' (2013) 26 *Leiden J of Intl L* 793, concluding that 'the Manual reduces uncertainty through consensus on some issues, but also reproduces or even radicalizes uncertainty' by making 'authoritative claims in the absence of consensus' and reintroducing 'open-ended principles and contextual factors in legal reasoning'. See also François Delerue, *Cyber Operations and International Law* (CUP 2020) 35 (defining cyber operation as '[A] generic term used to describe acts taking place in cyberspace') and Ducheine and Pijpers (Ch 13 of this Handbook).

[7] According to the Tallinn Manual 2.0 (n 6) Rule 32 (168), cyber espionage means 'any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather, or attempt to gather, information. Cyber espionage involves, but is not limited to, the use of cyber capabilities to surveil, monitor, capture, or exfiltrate electronically transmitted or stored communications, data, or other information.' For a detailed analysis see Russell Buchan, *Cyber Espionage and International Law* (Hart 2018), 13 et seq, who defines cyber espionage 'as the non-consensual use of cyber operations to penetrate computer networks and systems with the objective of copying confidential data that is under the control of another actor' (27). See also Weissbrodt (n 4) 370–1; Buchan and Navarrete (Ch 11 of this Handbook).

[8] On the question of whether cyber manipulation amounts to a cyber attack see James E McGhee, 'Cyber redux: The Schmitt Analysis, Tallinn Manual and US cyber policy' (2013) 64 *J L & Cyber Warfare* 100.

[9] On the different understandings of 'cyber warfare' in State practice Cordula Droege, 'Get off my cloud: Cyber warfare, international humanitarian law and the protection of civilians' (2012) 94 *Intl Rev of the Red Cross* 533, 536–7. According to Delerue (n 6) 39 'The term ... is construed from the prefix "cyber", which refers to the relationship between the Internet and computer technology ... and ... "warfare" [that] can be defined as an armed conflict'. On computer network exploitation (CNE) and com-

i.e., the use of technical means to wage war against an adversary in cyberspace.[10] The reason for the focus on cyber attacks in this contribution is that only these forms of attacks are normally serious enough to qualify as international crimes and thus be covered by an international criminal jurisdiction like the International Criminal Court (ICC).

However, the exact meaning of a cyber attack is still subject of discussion.[11] Following the majority view three elements may be distinguished. First, a cyber attack is not carried out for (direct) financial gain or profit as are classical economic cyber crimes.[12] Secondly, the attack is not conducted for the purpose of gaining information ('cyber espionage').[13] Thirdly, a cyber attack alters, disrupts, degrades or destroys a computer network and may lead to a disruption of devices connected to the network under attack.[14] The latter element is well captured by the definition provided for by the (revised) Tallinn Manual: 'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[15]

In this context it needs to be debated whether *data damage* which causes malfunctions but falls short of physical damage in terms of hardware etc. should be captured by the above definition, especially taking into account its third element.[16] The drafters of the Tallinn Manual

puter network defence (CND) see Nils Melzer, *Cyberwarfare and International Law* (UNDIR Resources 2011) 5, https://unidir.org/publication/cyberwarfare-and-international-law accessed 6 Oct. 2021.

[10] See Lin (n 3) 519, discussing the differences between traditional warfare and cyber warfare regarding the law of armed conflict; Droege, ibid., 538, referring to 'cyber operations amounting to or conducted in the context of armed conflict'; also Melzer (n 9) 4; Heather H Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012) 4 et seq.

[11] *Cf* Ryan McClure, 'International adjudication options in response to state-sponsored cyber-attacks against outer-space satellites' (2012) 18 *New England J of Intl and Comparative L* 431, 432 (with further references).

[12] Melzer (n 9) 21; Lesley Swanson, 'The era of cyber warfare: Applying international humanitarian law to the 2008 Russian-Georgian cyber conflict' (2010) 32 *Loyola Los Angeles Intl & Comparative L J* 303, 307, '[cybercrimes] are governed by national criminal statutes and include such acts as identity theft and internet fraud'.

[13] Lin (n 3) 519; see also Jack Goldsmith, 'How cyber changes the laws of war' (2013) 24 *EJIL* 129, 135.

[14] This is basically the US Department of Defense definition, as quoted in Noam Lubell, 'Lawful targets in cyber operations: Does the principle of distinction apply?' (2013) 89 *Intl L Studies* 252, 258; see also Melzer (n 9) 5; Lin (n 3) 518–9; Brian T O'Donnell and James Kraska, 'Humanitarian law: developing international rules for the digital battlefield' (2003) 8 *J of Conflict and Security L* 133, 138; crit. of the scope of the definition Lubell, ibid., 258–9.

[15] Tallinn Manual 2.0 (n 6) Rule 92 (415) (note that this definition is inspired by the 'conduct of hostilities' definition of Art. 49 AP I); for an even broader definition Lin (n 3) 518–9; see also Droege (n 9) 556–61, including the interference 'with the functioning of an object by disrupting the underlying computer system', at 560); for a too broad (albeit called 'narrow') definition see Hathaway et al (n 4) 826 et seq., letting suffice 'any action … to undermine the functions of a computer network …'. Why the authors themselves consider this a 'narrow' definition remains their secret, the special purpose requirement ('political or national security purpose') does, in any case, not do the trick and their examples are also far too broad (ibid., 837 et seq.). Discussing different cyber operations and attacks Charlotte Lülf, 'International humanitarian law in times of contemporary warfare – the new challenge of cyber attacks and civilian participation' (2013) 26 *Humanitäres Völkerrecht – Informationsschriften* 74, 76–7.

[16] Tallinn Manual 2.0 (n 6) Rule 92 (415); see also below nn 48 et seq. and main text to malfunctions of critical infrastructures.

continue to be divided, although they move in the direction of affirming the question.[17] The gist of the issue is whether a 'replacement of physical components' is required to assume a physical damage or a 'reinstallation of the operating system or of particular data' suffices.[18] The latter view is more convincing. While data and objects are different, they are inseparably connected. For this reason, modern cyber attacks can already have an effect comparable to physical damage through functionally impairing data corruption, which in turn has a significant negative impact on cyberinfrastructures. A more restrictive view would take a considerable number of cyber attacks out of the definition and offer no normative protection with regard to the effects produced by such attacks.[19]

(b) Focus on Criminal Responsibility

The second limitation concerns the concept of 'international criminal responsibility'. Such a responsibility presupposes the existence of international crimes and the participation in these crimes. The current debate is mostly concerned with the application of the law of armed conflict, also – more euphemistically – called international humanitarian law (IHL),[20] to cyber attacks and the ensuing question when such attacks qualify as *war crimes* (thereto below section 2).[21] This is not surprising since States are, pursuant to Article 36 of the First Additional Protocol to the Geneva Conventions (AP I), under an obligation to determine the applicable IHL rules for new weapons and means or method of warfare.[22] The Tallinn Manual 2.0 now explicitly recognizes individual and superior (criminal) responsibility for war crimes.[23]

Less intense is the debate regarding criminal responsibility for the *crime of aggression* (section 3). This is equally unsurprising since this crime has only recently been codified and it

---

[17] Cf Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013) Rule 30 (109), only 'a few experts' in favour, focusing on the 'object's loss of usability', with the Tallinn Manual 2.0 (n 6) 415, Rule 92, mn. 11:

> Some … Experts … further took the position that interference with functionality extends to situations in which reinstallation of the operating system or of particular data is required in order for the targeted cyber infrastructure to perform the function for which it was designed. … If, as a result of a cyber operation deleting or altering data, the infrastructure cannot perform its intended function, the operation in question, in the view of these Experts, amounts to an attack.

[18] Tallinn Manual 2.0 (n 6) Rule 92 (415); Julia Dornbusch, *Das Kampfführungsrecht im internationalen Cyberkrieg* (Nomos 2017) 97–8.

[19] In the same vein see ibid.

[20] IHL refers to all rules of the law of armed conflict protecting individuals in armed conflicts (Mary Ellen O´Connell, 'Historical developments and legal basis' in Dieter Fleck (ed), *The Handbook of International Humanitarian Law* (OUP 2013) 1–43, marginal number ('mn.') 101) and to cases of declared war or occupation (Gerhard Werle and Florian Jeßberger, *Principles of International Criminal Law* (OUP 2020) mn. 1209–10).

[21] More on the application of IHL to the cyber realm can be read in Part IV of this Handbook.

[22] *Cf* Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks' (*International Committee of the Red Cross*, 19 November 2004) http://www.icrc.org/eng/resources/documents/misc/68lg92.htm accessed 6 Oct. 2021, 2; Droege (n 9) 540–41; Dinniss (n 10) 260–61; William H Boothby, 'Methods and means of cyber warfare' (2013) 89 *Intl L Studies* 387, 400.

[23] *Cf* Tallinn Manual 2.0 (n 6) Rule 84 (391), 'Cyber operations may amount to war crimes and thus give rise to individual criminal responsibility under international law' and Rule 85 (396–7), para (a) establishing the responsibility of 'Commanders and other superiors' for 'ordering cyber operations that constitute war crimes' and para. (b) for the failure 'to take all reasonable and available measure to prevent' such crimes 'or to punish those responsible'.

is much less likely that it will be applied any time soon to traditional armed attacks, let alone cyber attacks. Finally, there is virtually no debate regarding the commission of *crimes against humanity* by way of cyber attacks but it is worthwhile taking a brief look at this possibility following the discussion of war crimes (section 4).

There are, of course, other issues regarding international criminal responsibility in cyberspace but they must be left to future inquiries. One particularly complex and practically important topic concerns the question of jurisdiction for cyber attacks given that these attacks are by definition transnational and thus trans- or supra-jurisdictional. In fact, these attacks normally originate in one jurisdiction but concern all jurisdictions they cross and where they may produce harmful results. The ICC's jurisdiction would then be derived from the national jurisdiction(s) affected by the respective cyber attack. Serious issues arise when the deterritorialization of the cyberspace leads to a geographical disparity (transnationalization) of the origin (place of act), the perpetrator and the ensuing damage (place of result) of the cyber attack.[24]

2. CYBER ATTACKS AS WAR CRIMES

(a) Preliminary Remarks

War crimes are nowadays most comprehensively defined in Article 8 ICC Statute containing more than 50 individual offences all based on the primary prohibitions of the Hague and Geneva Laws.[25] Pursuing a structural and systematic approach focusing on the interests and rights protected one can distinguish between basic offences against protected persons and objects, attacks on civilian population and objects (prohibited means of warfare) and other offences (including prohibited methods of warfare).[26] Cyber attacks may constitute such offences if they meet their objective (*actus reus*) and subjective (*mens rea*) requirements. This cannot be determined in the abstract but depends on the concrete circumstances of each case. At any event, the application of the war crimes regime to any form of attack – be it by traditional kinetic or modern cyber means – is predicated on the existence of the general requirements for the application of IHL to the case at hand. Thus, these general requirements must be examined first before analysing how the traditional IHL principles play out in the field of cyber attacks.

---

[24] See Anne-Laure Chaumette, 'International criminal responsibility of individuals in case of cyber-attacks' (2018) 18 *Int Crim L Rev* 1, 23, giving three examples. In general Marco Roscini, 'Gravity in the Statute of the International Criminal Court and cyber conduct that constitutes, instigates or facilitates international crimes' (2019) 30 *CLF* 247, 249 et seq.

[25] On these primary rules see Kai Ambos, *Treatise on International Criminal Law. Volume I: Foundations and General Part* (OUP 2nd ed. 2021) 13 et seq.

[26] *Cf* Kai Ambos, *Treatise of International Criminal Law. Volume II: The Crimes and Sentencing* (OUP 2014) 164 et seq. (2nd ed. 2022 forthcoming).

(b) General Requirements

(i) Existence of an armed conflict[27]

According to Common Article 2 of the Geneva Conventions (GC),[28] the application of IHL is predicated on the existence of an armed conflict. The term is not positively defined in written IHL but the International Criminal Tribunal for the Former Yugoslavia (ICTY) has provided a generally accepted definition in its seminal *Tadić* (Jurisdictional Decision). Accordingly, 'an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State'.[29] Thus, what is of relevance is the employment of armed force and its attribution to one of the parties to the conflict.[30]

(1) Employment of armed force

The same principles apply to cyber attacks[31] as long as there is no specific definition of 'war' or 'armed conflict' for this kind of attack.[32] Thus, one should first of all distinguish between a situation where such an attack is part of an ongoing (conventional) armed conflict or where it is carried out independently of such a conflict (i.e., where such a conflict does not exist in the first place or only at a different time).[33] Given that in the former case the armed conflict

---

[27] See also Arimatsu (Ch 19 of this Handbook).

[28] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 21 October 1950) (GC I) 75 UNTS 31 (GC I); Convention II for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea. Geneva Field (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 85 (GC II); Convention relative to the Treatment of Prisoners of War Field (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135 (GC III); Convention relative to the Protection of Civilian Persons in Time of War Field (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 267 (GC IV).

[29] *Prosecutor v Tadić*, ICTY (Jurisdiction) IT-94-1-AR (2 October 1995) [Tadić Jurisdictional Decision] para 70; *Prosecutor v Lubanga* (Confirmation of Charges) ICC-01/04-01//06 (27th January 2007) para. 209; *cf* Werle and Jeßberger (n 20) mn. 1204; Antonio Cassese and others, *Cassese's International Criminal Law* (3rd ed, OUP 2013) 66.

[30] *Cf* Ambos (n 26) 123.

[31] Droege (n 9) 543 et seq.; Dinniss (n 10) 126 et seq.; generally more cautiously Lin (n 3) 515 et seq., concluding that many of the traditional IHL assumptions 'either are not valid in cyberspace or are applicable only with difficulty', at 530.

[32] See for an enlarged definition of the concept of 'war' Annex 1 of the Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security (adopted 16 June 2009) quoted in Melzer (n 9) 22 and Droege (n 9) 535. This Annex defines 'information war' as a:

> confrontation between two or more states in the information space aimed at damaging information systems, processes and resources, critical and other structures, undermining political, economic and social systems, mass psychologic brainwashing to destabilize society and state, as well as to force the state to taking decision in the interest of an opposing party.

[33] Dinniss (n 10) 127 et seq. distinguishes between three situations: during ongoing armed conflict, independent of such an armed conflict and accompanying conventional use of force not as such amounting to an armed conflict. The last situation may, however, be grouped together with the first since in both cases conventional armed and cyber attacks happen together with a lower degree of conventional force in the last situation. For Melzer (n 9) 24 cyber operations 'not accompanied by a threat or use of conventional military force' would normally not pass the armed conflict threshold but 'most likely be

threshold is passed anyway by the recourse to conventional armed force, the question of a separate assessment of the quality of a cyber attack arises only in the latter case of – what could be called – a 'pure' cyber attack (including a cyber attack on the occasion, but not in the context of an armed conflict).[34] In such a case it must be inquired whether armed force has been employed[35] and whether this can be attributed to one party to the conflict.

Whether armed force has been employed may be determined by looking at the means or instruments employed – 'means approach' – or at the effects, consequences or results generated by this employment – '(equivalent) effects approach'.[36] The former approach would have difficulties to consider a cyber attack as an 'armed' use of force since the computer systems employed to carry out such an attack cannot be considered 'arms' in the traditional sense since they lacking any kinetic expression of force.[37] In any case, such an approach does not only ignore the modern understanding of use of force which does not focus on the weapons employed.[38] It also fails to capture the special quality of cyber attacks which is not only expressed in the 'means of cyber warfare' (which may be qualified as 'cyber weapons')[39] but in particular in the effects of such attacks as compared to traditional (kinetic) armed attacks. Thus, one should follow the *effects approach*.[40]

---

regarded as a criminal threat to be addressed through law enforcement measures'. See also Delerue (n 6) 41 et seq.

[34] See on the necessary nexus between the armed conflict and the cyber operation below (b)(iii). However, it is meanwhile widely accepted that a cyber attack might reach the threshold of an armed conflict, see only Delerue (n 6) 41-2; Federal Government (of Germany), 'On the Application of International Law in Cyberspace' Position Paper (March 2021), https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf, accessed 1 Oct. 2021; thereto Michael N Schmitt, 'Germany's Positions on International Law in Cyberspace Part II', *Just Security* (10 March 2021), https://www.justsecurity.org/75278/germanys-positions-on-international-law-in-cyberspace-part-ii/ accessed 1 Oct. 2021.

[35] Insofar the difference between 'attack' (as defined in Art. 49 (1) AP I) and the broader concept of military 'operation' (see for e.g., Art. 51(1) AP I; for a discussion see Droege (n 9) 554 et seq.) is not relevant since in both situations armed force is employed. See with regard to the principle of distinction (Art. 48 AP I) however see text accompanying n 93 *infra*.

[36] The three relevant approaches (instrumentality-, target- and consequence-/effects-based) have been developed with regard to the *ius ad bellum* concept of an 'armed attack' (Art. 51 UN Charter) (see Hathaway and others (n 4) 845–6; Weissbrodt (n 4) 363–4) and are likewise used in the discussion about 'use of force' within the meaning of Art. 2 (4) UN-Charter (see Dornbusch (n 18) 66 et seq.) but can be applied in the *ius in bello* context of the armed conflict threshold as well.

[37] On the differences between traditional warfare and cyber warfare insofar see: Lin (n 3) 520 et seq.; see also Nils Melzer, 'Cyber operations and ius in bello' (2011) 4 *Disarmament Forum* 3, 5.

[38] *Cf Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226, para. 39, 'any use of force, regardless of the weapons employed'; conc. Tallinn Manual 2.0 (n 6) 328; Melzer (n 9) 13; Weissbrodt (n 4) 356; Boothby (n 22) 391; on the concept of weapon with a view to the military advantage achieved Dinniss (n 10) 68–70.

[39] *Cf* Tallinn Manual 2.0 (n 6) Rule 103 (452–3).

[40] See also Tallinn Manual 2.0, ibid., Rule 92 (415–6); see also p. 340-1 where in the context of the discussion of 'armed' attack the requirement of a use of weapons in the traditional sense is rejected focusing on the effects of a cyber operation; in the same vein Richard W Aldrich, 'The international legal implications of information warfare' (1996) 10 *Airpower Journal* 99; Dinniss (n 10) 74, 123, 131–2; Michael N Schmitt, 'Cyber operations and the jus in bello: Key issues' (2011) 87 *Intl L Studies* 89, 92 et seq.; Melzer (n 9) 7, 24; Emily Haslam, 'Information warfare: Technological changes and international law' (2000) 5 *J of Conflict Security L* 157, 170; Lülf (n 15) 77–8, also focusing on the effects of a cyber-operation and arguing that it reaches the threshold 'whenever' it 'endangers protected persons

An effects-based reading is not excluded by the definition of an 'armed attack' as 'acts of violence against the adversary' (Art. 49 (1) AP I). For 'violence' can also be brought about by the violent effects of a cyber attack producing a lasting harmful result.[41] Thus, if a cyber attack brings about the replacement of a physical part of an attacked computer network,[42] it reaches the armed force or armed attack threshold of IHL.[43] This confirms that the crucial issue is not the nature of the attack in terms of its means but of its effects. This entails, in contrast, that a cyber attack not causing any (lasting) physical or serious functional damage (e.g., a temporary shutdown/breakdown of a computer system) does not reach the armed conflict threshold.[44] Of course, the effects of an attack must be assessed in a broad sense. While a cyber attack may only produce limited damage on the attacked system as such the broader effects may nevertheless produce serious consequences, for example, if a large dam was regulated by this system and its deactivation entails widespread flooding. Thus, the question is always whether a cyber attack causes comparable or analogous damage to a traditional armed attack.[45]

In this regard, also the equal treatment of 'destruction, capture and neutralization' in Article 52(2) AP I seems to suggest a more flexible interpretation since it shows that neutralization of a military objective may produce a military advantage and thus may have the same effect as the destruction of this object.[46] Indeed, the drafters of Article 52(2) AP I had in mind that an attack 'for the purpose of denying the use of an object to the enemy' may have the same military effect as the destruction of this object.[47] In other words, a cyber operation leaving the targeted object physically intact but neutralizing it in its functionality may amount to a militarily relevant attack,[48] at least if the operation disables the 'critical infrastructure'[49] of

---

or objects' and 'is more than a sporadic and isolated incident'; Boothby (n 22) 389, 'critical factor … injurious or damaging effect ', 402; Dörmann (n 22) 3, 'degree of damage'; Lubell (n 14) 262–3, 265, 275, 'violent effects', 'harm caused'; Weissbrodt (n 4) 364, regarding armed attack; Hathaway and others (n 4) 845, 847–8; crit. because of a too high threshold Katherine C Hinkle, 'Countermeasures in the cyber context: One more thing to worry about' (2011) 37 *YJIL Online* 11, 11–2, 21, regarding the alleged Russian cyber-attack on Estonia in 2007; crit. because of uncertainties with regard to the concrete application Kessler and Werner (n 6) 808.

41 In the same vein Schmitt, ibid., 93–4; Melzer (n 9) 26.

42 Tallinn Manual 2.0 (n 6) Rule 92 (415–6).

43 Schmitt (n 40) 93; see also Yoram Dinstein, 'Computer network attacks and self-defense' (2002) 76 *Intl L Studies* 99, 103; Melzer (n 37) 7.

44 Melzer (n 37) 7; Schmitt (n 40) 95; similar: Swanson (n 12) 323; more detailed Tallinn Manual 2.0 (n 6) Rule 91 (415–6).

45 Droege (n 9) 546.

46 *Cf* Dörmann (n 22) 4, 6; crit. Schmitt (n 40) 95–6, warning of over-inclusivity and arguing that Art. 52(2) AP I is predicated on the existence of an 'attack' and that may exclude mere cyber-operations; Dinniss (n 10) 197–8; for a nuanced approach Melzer (n 9) 26, arguing that both positions have strong points.

47 *Cf* Droege (n 9) 558.

48 Ibid., 559, 'operations that disrupt the functioning of objects without physical damage or destruction, even if the disruption is temporary'; see also Boothby (n 22) 389–90, arguing, with regard to 'data', that it 'only becomes an "object" when it is critical to the operation of the targeted system'; Lubell (n 14) 265–6, criticizing an exclusive focus on physical damage.

49 According to sec. 2 of the US Executive Order of 12 Febr. 2013 a 'critical infrastructure' 'means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters', https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity?;

the respective State.[50] Of course, minor disruptions, like the shutdown of a TV broadcasting system, do not constitute military attacks; in fact, they normally cause less inconvenience than economic or psychological warfare[51] and these do not fall under the definition of an attack.[52] Articles 51(5)(b), 57(2)(a)(iii) and 57(2)(b) AP I confirm this view since they only mention physical consequences of armed attacks.[53]

One may however come to a different conclusion focusing, in line with the *target-based* approach, on the nature and importance of the target as the object of a cyber attack. This approach takes into account the attack's impact on (critical) infrastructures[54] and thus stresses an important feature of cyber attacks:[55] these kinds of attacks do not need to cause a huge physical damage to have a significant impact. Even data damage causing disruption in terms of the functionality of critical infrastructure can have this impact and may therefore, as already argued above,[56] amount to a cyber attack. From this perspective, an attack, that causes only little physical damage or just a virtual damage but hits a critical target may also amount to a 'use of force' or an 'armed attack'.[57] A *combination of the target-based with the effects based approach* may produce a useful guideline: if the effects of a cyber attack for the critical infrastructure are highly significant due to the importance of the target attacked the cyber attack may, on the whole, amount to an armed attack.[58] Clearly, such attacks are much more serious

---

was still relevant under Trump: https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-strengthening-national-resilience-responsible-use-positioning-navigation-timing-services/; Biden announces further protection https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/ all accessed 6 Oct. 2021.

[50] On this criterion with definitions (regarding *ius ad bellum*) Melzer (n 9) 14–16.

[51] Schmitt (n 40) 95; in a similar vein ibid., 26.

[52] Droege (n 9) 559; see also Boothby (n 22) 403, emphasizing that 'only death, injury, damage or destruction to protected persons or objects' should be considered; Tallinn Manual 2.0 (n 6) 418, 'cyber operations that merely cause inconvenience or irritation' no attack; with respect to State practice Schmitt (n 40) 95, 103.

[53] Michael N Schmitt, 'Wired warfare: Computer network attack and ius in bello' (2002) 84 *Intl Rev of the Red Cross* 365, 377–8.

[54] Focarelli defines critical infrastructures 'as the assets that are essential for the functioning of a society and economy, notably for the supply of essential services' and gives multiple examples; Focarelli (Ch 15 of this Handbook).

[55] Walter Sharp, *Cyberspace and the Use of Force* (Aegis 1999) 129–30; Eric T Jenson, 'Computer attacks on critical national infrastructure: a use of force invoking the right of self-defense' (2002) 38 *Stan J Intl L* 207, 226; for a good comparison see Nguyen (n 5) 1119 et seq.; also Tallinn Manual 2.0 (n 6) 418, 'few Experts' pointing to 'loss of usability of cyber infrastructure'.

[56] See (n 16) and main text.

[57] Dornbusch (n 18) 101–2; for the same view Ministère des Armées (Ministry of the Armies), Droit International Appliqué aux Opérations dans le Cyberspace, Sept. 2019, referring to a relevant impact on French defensive capabilities, https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqué+aux+opérations+Cyberespace.pdf accessed 6 Oct. 2021. Crit. Delerue (n 6) 288 arguing that the approach is too 'inclusive'.

[58] See thereto Luca Petersen, 'Cyberangriffe - Definition, Regulierung, Pönalisierung' (2020) 3 Goettinger Rechtszeitschrift 25, 30; in favour, however, of a combination of the instrument-based (focusing on the used instrument) and effect-based approach, Marco Roscini, Cyber Operations and the Use of Force in International Law (OUP 2014) 50; thereon Delerue (n 6) 289-91 (also in favour of the effect-based approach, taking into account the other two approaches).

than cyber espionage or manipulations. Take as a recent example the US cyber attack on an Iranian military database.[59]

In sum, pursuant to the effects approach, a cyber attack as defined above, i.e., as an attack causing considerable human and other damage or a serious disruption of a computer system, will normally amount to the employment of armed force and thus constitute a militarily relevant attack.[60] Of course, the amount of casualties alone does not turn a conflict into an armed conflict,[61]the quality of the attacks – against protected persons and objects – always plays an important role in assessing the nature of the conflict.[62]This speaks in favour of a combination of different factors, the effects being the most important one, but nature of the target and means of the attack to be taken into account.[63] The same test can be applied with regard to the necessary intensity and duration – 'protracted armed violence'[64] – of a (non-international) armed conflict[65] which presupposes a series of attacks lasting a considerable amount of time.[66] It is questionable, however, whether, in addition, a specific intent to cause injury and destruction, the foreseeability of these consequences should also be required.[67] While such a 'subjectification' may further restrict the effects criterion and in particular avoid a mere quantitative assessment,[68] it seems to conflate the per se objective armed conflict/attack threshold with the requirements of individual criminal responsibility and thus appears theoretically incoherent. In addition to that, it would also entail difficult evidentiary problems.

---

[59] See on this Edwin Djabatey, Reassessing U.S. cyber operations against Iran and the use of force, 17 Oct. 2019, https://www.justsecurity.org/66628/reassessing-u-s-cyber-operations-against-iran-and-the-use-of-force/, accessed 6 Oct. 2021:

> From what is publicly known about the operation, it was 'intended to take down the computers and networks used by the … group, at least temporarily.' It 'wiped out a critical database' used by the IRGC to plan attacks against ships in the Gulf, leaving Iran attempting to restart the affected computer systems and recover the information lost. In this way it apparently 'diminished Iran's ability to conduct covert attacks'.

[60] Schmitt (n 53) 374; Droege (n 9) 545 et. seq., 560, 578; Dinniss (n 10) 123, 131, 137–8, threshold of 'significant seriousness'; Melzer (n 37) 5; Droege (n 9) 14, critical towards the requirement of consequence equal to traditional armed attacks; Tallinn Manual 2.0 (n 6) Rule 92 (415); Haslam (n 40) 170; Swanson (n 12) 314–15.

[61] Jean Pictet (ed), *Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* (1952, ICRC reprint 2006) [Pictet, GC I] 32, 'It makes no difference how long the conflict lasts, or how much slaughter takes place'.

[62] Schmitt (n 53) 373.

[63] On such a combined approach Droege (n 9) 547–8.

[64] *Cf Tadić Jurisdictional Decision* (n 29) para. 70; incorporated in Art. 8 (2)(f) ICC Statute (adopted 17 July 1998, entered into force 1 July 2002, 2187 UNTS 3); see also Schmitt (n 40) 106.

[65] *Cf* Droege (n 9) 551.

[66] Melzer (n 9) 24–5, arguing that the precise threshold has not yet been defined; Dinniss (n 10) 131. For Hathaway and others (n 4) 850 and Robin Geiss, 'Cyber warfare: Implications for non-international armed conflict' (2013) 89 *Intl L Studies* 627, 633–4, the necessary threshold has not yet been reached in practice by an isolated cyber attack. Kessler and Werner (n 6) 800 generally point out that there has been, apart from the Stuxnet attack, 'no incident of cyberwar that inflicted the widespread devastation and damage usually associated with "war"'.

[67] In this sense Schmitt (n 53) 374, 'either intended to cause injury, death, damage or destruction … or such consequences are foreseeable'; also Schmitt (n 40) 94–5; emphasizing the intention of the attacker also Dinniss (n 10) 132–3.

[68] In this vein Melzer (n 9) 16.

(2) Attribution to a party to the conflict

The second requirement – the attribution of a cyber attack to one of the parties to the conflict – may be more difficult to fulfil. Attribution is practically impossible if the attacker cannot be identified, i.e., the attack comes out of the anonymity of the World Wide Web and cannot be traced back to a specific user belonging to a party to the conflict;[69] it may also be traced mistakenly to a wrong person who was just used as an innocent messenger.[70]

But even if the attack is carried out by identifiable individuals or groups, the question arises whether they themselves are parties to a (non-international) armed conflict or whether their acts can be attributed, pursuant to Article 4A(2) GC III ('belonging to a Party'), to a party to an (international) armed conflict, in particular a State.[71] As to the former question, the answer depends on a sufficient degree of organization of these groups, i.e., the required command, control, discipline and hierarchy characteristic for IHL armed groups;[72] they may then be parties to a non-international armed conflict.[73] However, groups of persons ('hackers') with a mere virtual existence normally lack these features;[74] also, a spontaneous collective attack (like a denial-of-service attack) finding more and more online followers, does not comply with the organization requirement.[75]

As to a possible attribution of the acts of these groups to a State the ILC's rules on State responsibility for wrongful acts[76] provide a useful guidance.[77] Also, the ICRC Interpretive Guidance is helpful requiring, 'at least a *de facto* relationship between an organized group and a Party to the conflict'.[78] Accordingly, the fact that a 'rough' State may always lay blame for a cyber attack from its territory on private hackers in order to elude its State responsibility[79] is not relevant in this context since the existence of an armed conflict with the respective parties will be determined objectively.

---

[69] *Cf* Droege (n 9) on the problems of attribution in light of the anonymity of the attacker (541, 543–5); see also Goldsmith (n 13) 131–2, 134; Hinkle (n 40) 17–8; Dinniss (n 10) 99–102; Kessler and Werner (n 6) 799.

[70] *Cf* Tallinn Manual 2.0 (n 6) 420, 'unwittingly' forwarding email with malware.

[71] Apart from States only national liberation movements can be a party to an international armed conflict pursuant to AP I, see e.g., Art. 96(3) which gives them the possibility to make a unilateral declaration regarding the application of IHL.

[72] See for the definition Ambos (n 26) 125–6; in our context Schmitt (n 40) 105–6; Geiss (n 66) 634; Dinniss (n 10) 124–5.

[73] *Cf* Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (ICRC 2009) 24 [hereinafter 'ICRC Interpretive Guidance'].

[74] Droege (n 9) 550–1; Geiss (n 66) 635–6; Melzer (n 9) 24; for a different view apparently Michael N Schmitt, 'Classification of cyber conflict' (2012) 17 *J of Conflict Security* L 245, 256, arguing that 'such groups can act in a coordinated manner against the government … take orders from a virtual leadership, and be highly organized'.

[75] Geiss (n 66) 635.

[76] *Cf* ILC, Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries (2001) Report of the ILC, 53rd Session (23 April to 1 June and 2 July to 10 August 2001) UN Doc A/56/10 (2001) 20, Arts 4–9, establishing the rules of attribution of acts of State organs or private groups or agents to a State. On the effective vs. the overall control test (*ICJ Nicaragua vs. ICTY Tadić*) in this context see Schmitt (n 40) 104–5. Discussing possible ('reciprocal') countermeasures Hathaway and others (n 4) 857–9; Hinkle (n 40) 14 et seq.; regarding the ius in bello Dinniss (n 10) 75 et seq.

[77] Droege (n 9) 544.

[78] lCRC Interpretive Guidance (n 73) 23; conc. Tallinn Manual 2.0 (n 6) 403–4.

[79] *Cf* Goldsmith (n 13) 135.

(ii) Geographical scope of the armed conflict

In an international armed conflict between two or more States the hostilities take normally place in these States or at least in one of them (e.g., in case of an invasion in this State). As to a non-international armed conflict Common Article 3 GC I-IV requires the conflict to take place 'in the territory of one of the High Contracting Parties'. Other provisions[80] and the international case law confirm that there must be a territorial link or nexus of some sort. The *Tadić* Jurisdictional Decision referred to armed violence 'within a State'[81] and the ICC *Bemba* PTC to 'the confines of a State territory'.[82]

However, cyber attacks defy any geographical limits by State territories or borders.[83] They may originate in a mobile device moving between different States, pass through a server or servers located in other States and finally hit the target in yet another State. If each device or network involved in a cyber attack would become a targetable military objective this would entail a kind of 'total cyber war' breaking up any traditional geographical limits of the battlefield[84] with 'far-reaching destabilizing effects on relations between States'.[85] Focusing on the effects of a cyber attack[86] does not mitigate the risk of such an extension of cyber violence since counter-attacks would always target those computers, devices or networks that caused the said effects, and would probably spread over different territories. A limitation would only be possible if the cyber attack could be traced back to the computer or device where it originated and if only this could be a lawful target of a counter-attack.

This shows that virtual cyberspace is connected to the 'real world' via the (necessary) physical hardware.[87] Geographical allocation is therefore possible in principle, especially in the case of high sensitive data storage.[88] It becomes highly problematic if the data used by the hardware is located on another data storage device – which is located in another country – and is accessed, for example, by a cloud.[89] At any rate, in the case of disruption of functionality there will be a link between the data and the territory where the physical hardware is located.

---

[80] *Cf* Art. 1 AP I, and relating to the Protection of Victims of Non-International Armed Conflicts (adopted 12 December, entered into Force 7 December 1978) 1125 UNTS 609 [AP II], Art. 8(2)(f) ICC Statute.

[81] *Prosecutor v Tadić*, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1 (2 October 1995), para. 70. See also *Prosecutor v Blaskić* (Judgement) IT-95-14-T (3 March 2000) paras 63–64; *Prosecutor v Hadžihasanović and Kubura* (Judgement) IT-01-47-T (15 March 2006) para. 14; *Prosecutor v Limaj et al.* (Judgement) IT-03-66-T (30 November 2005) para. 84; *Prosecutor v Milutinović et al.* (Judgement) IT-05-87-T (26 February 2009) para. 127; *Prosecutor v Perišić* (Judgement) IT-04-81-T (6 September 2011) para. 72.

[82] *Prosecutor v Bemba* (Confirmation of Charges) ICC-01/05-01/08 (15 June 2009) para. 231; conc. *Bemba* (Trial Judgment) ICC-01/05-01/08 (21 March 2016) para. 128.

[83] Geiss (n 66) 631, 637; Goldsmith (n 13) 131.

[84] Droege (n 9) 565–6.

[85] Geiss (n 66) 640.

[86] Dinniss (n 10) 135.

[87] Dornbusch (n 18) 28.

[88] Sven-Hendrik Schulze, *Cyber-"War" – Testfall der Staatenverantwortlichkeit* (Mohr Siebeck 2015) 111.

[89] Ibid.

(iii) Nexus between a cyber attack and the armed conflict

Under conventional IHL the respective war crime must be related to the armed conflict.[90] This so-called nexus requirement has been interpreted broadly though, i.e., a *functional relationship* between the respective acts and the conflict suffices, but the respective crimes must not be committed merely on the occasion of the armed conflict, taking advantage of the resulting chaos.[91] To determine the nexus a series of factors may be taken into account.[92]

It is clear that a cyber attack also requires such a nexus with an ongoing armed conflict.[93] It can be taken to exist if, as under conventional IHL,[94] the perpetrator would not have been able to carry out the attack without the armed conflict.

(iv) Responsible agent

Any person, including a private contractor, acting on behalf of one of the parties to the conflict, can commit a war crime.[95] As already mentioned above,[96] the Tallinn Manual 2.0 explicitly recognises individual and superior (criminal) responsibility for war crimes; it basically draws on Articles 25 and 28 ICC Statute but includes an active 'ordering' responsibility of the superior in its command responsibility provision. In the cyber context the participation of civilians is of particular relevance since, especially in this area, the recourse to and the reliance on civilian expertise is indispensable.[97] These civilians may be formal members of the armed forces, including of irregular forces within the meaning of Article 4A(2) GC III (belonging to a party to an international armed conflict), or participants in a '*levée en masse*';[98] as such they

---

[90] *Tadić Jurisdictional Decision* (n 29) para. 70; *Prosecutor v Aleksovski* (Judgement) IT-95-14/1-T (25 June 1999) para. 45; *Prosecutor v Musovic et. al.* (Judgement) IT-96-21-T (16 November 1998) para. 193; see also Werle and Jeßberger (n 20) mn. 1226 et seq. (with further references).

[91] Ambos (n 26) 141.

[92] *Prosecutor v Kunarac, Kovac and Vokovic* (Appeals Judgement) IT-96-23 & IT-96-23/1-A (12 June 2002) para. 59:

> take into account, inter alia, the following factors: the fact that the perpetrator is a combatant; the fact that the victim is a non-combatant; the fact that the victim is a member of the opposing party; the fact that the act may be said to serve the ultimate goal of a military campaign; and the fact that the crime is committed as part of or in the context of the perpetrator's official duties.

Concurring *Prosecutor v Katanga and Ngudjolo Chi* (Confirmation of Charges) ICC-01/04-01/07-717 (30 September 2008) para. 382.

[93] Tallinn Manual 2.0 (n 6) Rule 80 (376); Melzer (n 9) 23.

[94] See in this regard Werle and Jeßberger (n 20) mn. 1227.

[95] Jean Pictet (ed), *Commentary on the Geneva Convention relative to the Protection of Civilian Persons in Time of War* (1958, reprint 1994) 212; Werle and Jeßberger, ibid., mn. 1231; Tallinn Manual 2.0 (n 6) Rule 84 (391 et seq.).

[96] Above n 23.

[97] Turns (n 2) 289–90, with a useful distinction of the tasks to be fulfilled; Hathaway and others (n 4) 854; Lülf (n 15) 79.

[98] *Cf* Art. 4A(6) GC III and Tallinn Manual 2.0 (n 6) Rule 88 (408-9); also 428 (targetability of participant in *levée en masse*).

possess combatant[99] and POW status.[100] Contracted personnel may however be assimilated to mercenaries thereby losing combatant and POW status ('unprivileged belligerents').[101]

These civilians may also be members of organized armed groups participating in a non-international armed conflict[102] and thus lose their civilian status *qua* this membership[103] which in turn makes them targetable, either pursuant to their 'continuous combat function'[104] or pursuant to their mere status (as members of an organized armed group).[105] Otherwise, civilians lose immunity from attack in a non-international armed conflict if they take 'direct part in hostilities'.[106] This is generally the case if they fulfil three minimum requirements:[107] (1) the respective act must negatively affect the adversary's military capacity or inflict substantive harm on him (threshold of harm); (2) a direct link between the act and the harm inflicted exists (direct causation); (3) the act must be related to the hostilities (belligerent nexus).[108]

These criteria can also be applied in the cyber context although some cyber-specific questions exist, for example, how cyber active civilians should distinguish themselves from ordinary civilians.[109] Direct participation depends, of course, on the circumstances of the specific case[110] but a clear-cut example would be a civilian preparing and activating a virus to be sent to the computer network of another State and causing significant (infrastructure) damage since in this case the civilian would actually conduct a cyber attack.[111] Also, a direct participation would generally exist if the attack would not have been possible without the special expertise

---

[99] This cuts both ways: they would then benefit from the combatant privilege (immunity from prosecution for lawful acts of war) but would also be lawful target, i.e., lose civilian immunity (targetability).

[100] In the case of Art. 4A(2) GC III they must fulfil the four requirements indicated there; see generally Melzer (n 9) 34; Turns (n 2) 290; Dinniss (n 10) 140 et seq. These requirements fulfil the customary international law criteria for combatancy, *cf* Tallinn Manual 2.0 (n 6) Rule 87 (402).

[101] *Cf* Art. 47 AP I and Tallinn Manual 2.0, ibid., Rule 90 (412–3); see also Dinniss (n 10) 172–5; Turns (n 2) 294.

[102] ICRC Interpretive Guidance (n 73) 31–2; conc. Schmitt (n 40) 98. On the criteria see already *supra* Ambos (n 26) with main text.

[103] ICRC Interpretive Guidance, ibid., 27–8; Tallinn Manual 2.0 (n 6) Rule 91 (414).

[104] ICRC Interpretive Guidance, ibid., 27, 33–5.

[105] The experts of the Tallinn Manual were divided on the issue, *cf* Tallinn Manual 2.0 (n 6) Rules 96 (b) (426).

[106] *Cf* Arts 3 GC I-IV, 51(3) AP I, 13(3) AP II and Tallinn Manual 2.0, ibid., Rule 91 (413-4), Rule 97 (428 et seq.). See also Bannelier (Ch 20 of this Handbook).

[107] These are criteria which resulted from the ICRC consultation process, *cf* ICRC Interpretive Guidance (n 73) 46; conc. Schmitt (n 40) 101; Dinniss (n 10) 165–6; see also Ambos (n 26) 156; Turns (n 2) 286. They have also been adopted by the Tallinn Manual 2.0 (n 6) Rule 97 (429–30). For a more thorough treatment see Dinniss, ibid., 161 et seq.

[108] This last criterion rules out purely criminal conduct, *cf* Tallinn Manual 2.0, ibid., Rule 97 (430).

[109] *Cf* Melzer (n 9) 29–30; Dinniss (n 10) 145 et seq. (especially referring to Art. 44(3) AP I); see also David Wallace, Shane Reeves & Trent Powell, 'Direct Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines' (2021) 12 *Harv. Nat'l Sec*. J. 164, 187 et seq.

[110] For a discussion see Turns (n 2) 286–9, 294–5, demonstrating the uncertainty of these criteria and presenting a useful table with possible examples.

[111] Tallinn Manual 2.0 (n 6) Rule 97 (430) with further examples; see also Lin (n 3) 526; Dinniss (n 10) 167.

of the civilian.[112] In contrast, there would be no direct participation if the civilian only possesses a merely inferior support function[113] or if he only makes malware available online.[114]

Here again the issue arises, already discussed above with regard to the attribution requirement, how to treat a group of hackers which organizes a spontaneous resistance activity and attacks the computer networks of an occupying force? Does such a group of persons qualify as an organized armed group as defined above and could for that reason be attacked?[115] Or could their acts be attributed to a party to the conflict? Or does such an activity amount to a '*levée en masse'* mentioned above? This would require consideration of the computers or software of the hackers as 'arms' carried 'openly' (Art. 4A(6) GC III) and their conduct as a spontaneous act of resistance.[116]

Finally, as to the duration of the participation ('for such time') and a (definite) withdrawal of a cyber participant the traditional problems[117] are even magnified in the cyber context. If one would consider it sufficient that a cyber participant interrupts his activity for a moment – parallel to a (temporal) withdrawal from the battlefield ('revolving door' problem) – it would become practically impossible to counter-target him since the actual cyber attack only lasts minutes and the virtual battlefield, in any case, may be the private PC of the hacker in his apartment. It is for this reason that the duration of the participation should last as long as the cyber participant engages in repeated cyber operations.[118]

(c) IHL Principles

The commission of a concrete war crime depends to a large extent on the understanding of the traditional IHL principles, i.e., the principles governing the conduct of hostilities,[119] in particular the principles of distinction, proportionality and precaution.[120] This is not different

---

[112] *Cf* ICRC Interpretive Guidance (n 73) 53, 'where the expertise of a particular civilian was of very exceptional and potentially decisive value for the outcome of an armed conflict …'.

[113] Louise D Beck, 'Some thoughts on computer network attack' (2002) 76 *Intl L Studies* 163, 171, arguing that technicians 'that actually undertake the attacks' would be considered civilians taking direct part in hostilities and would therefore be subject to counter-attack without the right to POW status pursuant to Art. 4 (4) GC III; conc. Dörmann (n 22) 9, 'executing' a CNA versus mere maintenance of computer networks; Turns (n 2) 293; for a more nuanced approach Dinniss (n 10) 167–72, excluding only 'routine systems maintenance'.

[114] Tallinn Manual 2.0 (n 6) Rule 97 (430); Wallace (n 109) 188.

[115] See for a discussion Schmitt (n 40) 98–101, identifying as the hard cases the ones of persons acting with a common purpose.

[116] Rather sceptical Turns (n 2) 293; see also Melzer (n 9) 34, discussing how the requirement of 'carry arms openly' should be interpreted.

[117] *Cf* Ambos (n 26) 157 et seq.

[118] Schmitt (n 40) 102; the issue was controversial within the Tallinn expert group, *cf* Tallinn Manual 2.0 (n 6) Rule 97 (432).

[119] According to the ICRC, 'the concept of "hostilities" refers to the (collective) resort by the parties to the conflict to means and methods of injuring the enemy, and could be described as the sum total of all hostile acts carried out by individuals directly participating in hostilities' (ICRC Interpretive Guidance (n 73) 43, 44).

[120] On the prohibition of perfidy see Art. 37 AP I and Tallinn Manual 2.0 (n 6) Rule 122 (491 et seq.), omitting the capture as a consequence of perfidy; on the difficult delimitation to lawful ruses in our context see Beck (n 113) 171; Dörmann (n 22) 10–12; Melzer (n 9) 32–3; Dinniss (n 10) 261–5, 278; Boothby (n 22) 404; see also Tallinn Manual 2.0 (n 6) 496, disagreement 'as to whether it would be

with regard to cyber attacks or, more broadly speaking, cyber operations[121] which qualify as 'hostilities' in this sense.[122] Thus, for example, to determine whether the war crime of an intentional attack on civilian objects (Art. 8(2)(b) (ii) ICC Statute) has been committed by way of a cyber attack, one must distinguish between civilian and military objects. Similarly, to decide whether a cyber attack causes disproportional collateral damage the meaning of proportionality in this context must be determined.

(i) Principle of distinction[123]

The distinction between, on the one hand, civilians and combatants and, on the other, civilian objects and military objectives lies at the heart of IHL and is embodied in Article 48 AP I.[124] It is 'part of customary international law applicable in both international and non-international armed conflicts'[125] and thus also applies to cyber attacks.[126]

The principle is often decisive in determining whether attacks on persons or objects qualify as war crimes or as lawful acts in armed conflict. While the civilian status of a person is, in case of doubt, presumed,[127] the customary status of the respective rule for objects[128] is controversial.[129] This controversy led the Tallinn Manual to adopt a compromise formula according to which, in the case of a military objective, a determination requires a 'careful assessment'.[130] At any rate, in both cases it is up to the attacker to 'do everything feasible to verify' the non-civilian (non-protected) nature of the targets.[131] As to civilians who are not

---

lawful to camouflage a computer or computer network to blend in with a civilian system in a manner that did not constitute perfidy'.

[121] These principles apply not only in the context of 'attacks' (within the meaning of Art. 49 (1) AP I) but also in the context of broader 'military operations' as clearly follows from Art. 51 (1) and 57 (1) AP I referring explicitly to the latter (*cf* Dinniss (n 10) 196 et seq.; in the same vein Droege (n 9) 555–6; Melzer (n 9) 27; stressing however the difference Schmitt (n 40) 91–3, arguing that 'operation' in Art. 48 AP I is to be understood as 'attack'; Lubell (n 14) 261; in a similar vein Tallinn Manual 2.0 (n 6) Rule 121 (487 et seq.), according to which the Rule required precautions with regard to cyber attacks, not all cyber operations, limiting thereby Art. 58(c) AP I as its base norm referring to 'military operations'.

[122] The threshold is lower than that for an 'attack' (Art. 49(1) AP I, supra note 40 and main text), *cf* Melzer (n 9) 28–9.

[123] See also Bannelier (Ch 20 of this Handbook).

[124] Art. 48 AP I reads:

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.

[125] Jean-Marie Henckaerts, Louise D Beck and Carolin Alvermann, *ICRC Study on Customary International Humanitarian Law, Volume I: Rules* (CUP 2005) [ICRC Study I], 25; see also ibid., rules 1–10 with pp 3 et seq.

[126] *Cf* Tallinn Manual 2.0 (n 6) Rule 93 (420 et seq.); Tilman Rodenhäuser, 'Hacking Humanitarians? IHL and the protection of humanitarian organizations against Cyber Operations', EJIL: *Talk!* (16 March 2020), https://www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyber-operations/ accessed 1 Oct. 2021.

[127] Art. 50(1) AP I and Tallinn Manual 2.0, ibid., Rule 95 (424). On the question of whether a presumption against direct participation is applicable see Wallace (n 109) 190 et seq.

[128] Art. 52(3) AP I.

[129] See discussion in Tallinn Manual 2.0 (n 6) 448–9 (regarding Rule 102).

[130] Ibid., Rule 102 (448).

[131] Ibid., Rule 115 (478).

formal members of the armed forces or an organized armed group, the question of 'direct participation' – independent of status – just discussed arises turning them eventually into military targets.

Given the above-mentioned controversy, it is not surprising that particular problems of delimitation arise with regard to the distinction between civilian objects and military objectives.[132] The term 'civilian object' is defined in Article 52 (1) AP I in a negative sense, i.e., as 'all objects which are not military objectives'.[133] Military objectives are 'limited to those objects which by their nature, location, purpose or use make an *effective* contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a *definite* military advantage'.[134] This is a two-pronged test with the terms 'effective' and 'definite' being most controversial. The ICRC defines the requirement of 'effective contribution' quite narrowly limiting it to purely military targets and excluding objectives of uncertain advantage.[135] A broader view, defended in particular by the US, includes attacks on targets which limit the enemy's war-fighting or war-sustaining capabilities.[136] Ultimately, the decision must be taken on account of the nature, location, purpose, or use of the target,[137] expressing a close nexus between the targeted object and military action.[138] Thus, the decision will always be context-related and on a case-by-case basis. For example, if combat takes place in a per se civilian area but civilian buildings like schools or churches are taken as cover by combatants or insurgents, those buildings turn into military objectives;[139] of course, absolute prohibitions, for example, regarding medical establishments,[140] must always be respected.[141]

Another question in this context is whether *data* can be considered a protected object. The mainstream position that the term 'objects' only covers tangible and visible objects and not data itself,[142] takes a too traditional approach relying on the old interpretation of the rule which had been developed when the possibility of cyber attacks must have appeared as mere science fiction. From a modern perspective the difference between physical and virtual objects becomes, at least in the cyber context, blurred; therefore, data should, in principle, be covered by the protection.[143] In any case, pursuant to the effects approach one has to look at the overall

---

[132] See generally with regard to the distinction between civilians (protected persons) and (de facto) combatants Ambos (n 26) 146 et seq.

[133] Tallinn Manual 2.0 (n 6) Rule 100 first sentence (435).

[134] Art 52(2) AP I (emphasis added) and Tallinn Manual 2.0, ibid., Rule 100 second sentence (435–6); for a discussion see Dinniss (n 10) 184 et seq.; see also Schmitt (n 52) 380; Geiss (n 66) 639–40.

[135] Claude Pilloud and others, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Nijhoff 1987) 636.

[136] *Cf* Art. 52(2) AP I; see also Schmitt (n 53) 381; crit. Droege (n 9) 567–8; Dinniss (n 10) 188–9.

[137] Stefan Oeter, 'Methods and means of combat' in Fleck (n 20) mn. 443, 'The formula used constitutes a general criterion the existence of which can be judged *in abstracto*'.

[138] *Cf* Droege (n 9) 562.

[139] Dörmann, '§ 11 VStGB' in Joecks and Miebach, *Münchener Kommentar zum Strafgesetzbuch*, (Vol. 8, 3rd ed, C.H. Beck 2018), mn. 54.

[140] *Cf* Art. 19 GC I, Art. 18 GC IV, Art. 12 AP I; see also Arts 54–56 AP I.

[141] For a comprehensive discussion of such prohibitions in our context see Dinniss (n 10) 220 et seq.; see also Dörmann (n 22) 6 et seq.

[142] Tallinn Manual 2.0 (n 6) Rule 100 (437); also Dornbusch (n 18) 94 et seq.

[143] In a similar vein Lubell (n 14) 267–8, 271; Melzer (n 37) 11; Melzer (n 9) 31 (both considering data as 'objects'); Dinniss (n 9) 184–5 (focusing on the aim or purpose of an operation); for an overview of the different views of experts and States see Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann,

harm caused instead of the isolated physical damage.[144] Given the already above-mentioned connection between (virtual) data and (physical) hardware (storage facilities) and other objects, especially of critical infrastructure, data damage will often also have consequences in the real (physical) world. Of course, there may not necessarily be a physical damage, but even a mere functional defect may have a relevant effect on the object. Thus, while (virtual) data differ from physical objects, there is an inseparable link between them, and this link allows the specific characteristics of data to be taken into account under the existing regulations on objects by focusing on the effects of data damage on the objects. At the same time, the principle of distinction comes into play when a cyber attack on civilian data simultaneously entails relevant effects on certain non-civilian objects.[145]

The key problem of the applicability of the principle of distinction is the *interconnectivity* between military and civilian computer systems and the mostly *dual-use* of cyber infrastructure.[146] Dual-use objects serve both civilian and military purposes but, as a matter of the law of armed conflict (i.e., a consequence of the principle of distinction), an object is either of a civilian or military nature.[147] In fact, as a rule, dual-use objects are qualified as military objectives since they normally contribute to military purposes, i.e., the first prong of the Article 52(2) AP I definition is fulfilled.[148] However, the alleged military contribution must effectively be demonstrated and cannot merely be presumed.[149]

Given that there is no clear-cut separation between civilian and military computer systems, i.e., that any computer system can be used for both civilian and military purposes at the same

---

'Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts' (2021) 102 *Intl Rev of the Red Cross* 287, 317 et seq.

[144] In the same vein Schmitt (n 40) 96; see also Robin Geiß and Henning Lahmann, 'Protection of Data in Armed Conflict' (2021) 97 *Intl L Studies*, 556, 562–3; Rodenhäuser (n 126) who highlights that the beneficiaries of humanitarian work are at risk.

[145] See e.g., the consequences of the worm Stuxnet, Gill (Ch 21 of this Handbook).

[146] Melzer (n 9) 30; Droege (n 9) 539, 541; Tallinn Manual 2.0 (n 6) Rule 121 (489); Turns (n 2) 296–7; Hathaway and others (n 4) 852–3; Goldsmith (n 13) 134; Dinniss (n 10) 193–5.

[147] *Cf* Tallinn Manual 2.0, ibid., Rule 101 (445), 'As a matter of law, status as a civilian object and military object cannot coexist; an object is either one or the other.'

[148] *Cf* ibid., 'confirms that all dual-use objects and facilities are military objectives, without qualification'; in the same vein Droege (n 9) 562–3.

[149] Dominik Steiger, 'Civilian objects', in Lachemann and Wolfrum (eds), *The Law of Armed Conflict and the Use of Force – Max-Planck-Encyclopedia of Public International Law* (OUP 2017), 208, 210 mn. 12:

> In the majority of cases, dual-use objects have to be considered military objectives. However, this is only true as long as the object makes an effective contribution to military action by its nature, location, purpose and use and if its destruction offers a definite military advantage in the circumstances ruling at the time.

ICRC Study I (n 125) 32, 'As far as dual-use facilities are concerned … practice considers that the classification of these objects depends, in the final analysis, on the application of the definition of military objective.'; William J Fenrick, 'Targeting and proportionality during the NATO bombing campaign against Yugoslavia' (2001) 12 *EJIL* 489, 494, '[It] is situation dependent. … [Dual-use] objects may become military objectives in certain conflicts depending on various factors, including the strategic objectives of the parties to the conflict and the degree to which the conflict approaches total war.' For a more nuanced view see also Robin Geiß and Henning Lahmann, 'Cyber warfare: Applying the principle of distinction in an interconnected space' (2012) 45 *Israel L Rev* 381, 389, arguing that, in the physical world, most civilian objects have no significant military potential and therefore cannot be used in a militarily conducive way.

time or interchangeably, the distinction is 'largely impossible' and, therefore, the protection offered by the principle of distinction of a limited practical importance.[150] Of course, this also depends on the broader or narrower reading of the principle and the particular circumstances of the case. In general, it seems quite plausible to argue that a per se civilian computer system loses its civilian status if 'it is used to make an effective contribution to military action'.[151] For example, if a conflict party uses a – per se civilian – information system of a hospital to launch cyber attacks these information systems may turn into military objectives.[152] It is more difficult to draw the line if one refers to a whole cyber infrastructure, including the internet. As the military relies to a large extent on civilian cyber infrastructure in all its operations,[153] including preparing and carrying out an attack, one may argue that this infrastructure per se – including the IT companies providing and supporting it or even social networks like Facebook or Twitter[154] – makes an effective contribution to the military effort and thus its destruction offers a definite military advantage.[155] Still more broadly one could argue that such a military use of civilian cyber infrastructure contaminates this infrastructure to a degree that it turns into a military objective. In this vein, the Tallinn expert group argues that in cases in which it is unclear, which internet connections are used for military transmissions, the whole network qualifies as a military target.[156] If one goes even further and let it suffice – contrary to the view defended here – that the military has the intent to use a civilian cyber infrastructure for military purposes in the future the whole civilian cyberspace would potentially constitute a legitimate military target.[157]

A further consequence of the principle of distinction is the *prohibition of indiscriminate attacks,*[158] although they differ from direct attacks against civilian objects in that the harm to the protected object does not matter to the attacker. It is questionable whether this prohibition can be complied with at all in case of cyber attacks to the same extent as in the case of traditional attacks. If, as argued above, a clear-cut separation between civilian and military cyber infrastructure is not possible, an attack against a cyber infrastructure can neither be considered clearly as an attack 'directed at a specific military objective' (Art. 51(4)) nor at a purely civilian object.

---

[150] Ibid., 383, 384–90; in the same vein Lucian E Dervan, 'Information warfare and civilian population: How the law addresses a fear of the unknown' (2011) 3 *Goettingen J of Intl L* 373, 388; Droege (n 9) 541, 562–6.

[151] Tallinn Manual 2.0 (n 6) Rule 102 (448).

[152] *Cf* Lin (n 3) 526.

[153] According to Dervan (n 150) 388, 'it is estimated that 98 percent of all classified governmental communications and 95 percent of all military communications in the United States flow through civilian communication systems, not dedicated military networks'.

[154] *Cf* Tallinn Manual 2.0 (n 6) Rule 101 (446–7); crit. Droege (n 9) 566–9.

[155] Geiß and Lahmann (n 149) 386, 388–9.

[156] Tallinn Manual 2.0 (n 6) (Rule 101) 446; *cf* ibid., (n 141) 388 et seq.

[157] Geiß and Lahmann (n 149) 386; Pilloud and others (n 135) 636.

[158] *Cf* Art. 51(4) AP I:

> Indiscriminate attacks are prohibited. Indiscriminate attacks are: (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

See generally ICRC Study I (n 125) rules 11–13.

Apart from that, the means used in a cyber attack, for example, a virus to be installed in a computer system, may not be sufficiently controllable, i.e., their effects cannot be – by definition – reasonably limited and thus cannot be discriminate.[159] Note however that in the case of the Stuxnet attack the virus was designed in a way that it only affected the systems of the Iranian nuclear program and its effects on civilian computer systems were negligible.[160] Under such a scenario the principle of distinction is not violated since, as mentioned above, data are no objects within the meaning of Article 48 AP I and they can only be treated alike if data damage affects (civilian) objects. Indeed, if this is the case the respective cyber attack qualifies as 'method or means of combat the effects of which cannot be limited'.[161] In fact, as correctly asserted by Droege, there is a twofold burden on the conflict parties: on the one hand, they may not employ cyber weapons that are indiscriminate by nature and cannot be sufficiently controlled; on the other hand, in each case of an attack the party has to verify whether the weapon employed can be and is in fact directed against a specific military target.[162]

In sum, the principle of distinction could only play a greater role if civil and military objects could be more clearly separated, for example, by the creation of 'digital safe havens' in analogy to demilitarized zones within the meaning of Article 60 AP I.[163] As the law currently stands the principles of proportionality and precaution, to be discussed in the following, may prove to be more useful to limit cyber attacks.[164]

(ii) Principle of proportionality[165]

The principle is part of customary international law in both international and non-international armed conflicts.[166] It sets limits to the use of means and methods of warfare and in particular prohibits causing 'superfluous injury or unnecessary suffering'[167] and 'widespread, long-term

---

[159] Boothby (n 22) 393–4; Beck (n 113) 169 called already more than ten years ago the limited control with regard to the effects of a CAN the 'most serious problem'; conc. Dörmann (n 22) 5; see also Dinniss (n 10) 256–7, discussing the issue under 'indiscriminate weapons'.

[160] For a discussion of Stuxnet see Gill (Ch 21 of this Handbook).

[161] *Cf* Art. 51(4)(c) AP I.

[162] Droege (n 9) 571.

[163] For a critical discussion of this and other possibilities see Geiß and Lahmann (n 149) 383, 390–5; see also ibid., 576–7.

[164] See also Tallinn Manual 2.0 (n 6) Rule 101 (445): 'An attack (Rule 92) on a military objective that is also used in part for civilian purposes is subject to the principle of proportionality (Rule 113) and the requirement to take precautions in attack (Rules 114–120)'; in the same vein Dervan (n 150) 388.

[165] See also Gill (Ch 21 of this Handbook).

[166] ICRC Study I (n 125), rule 14; Tallinn Manual 2.0 (n 6) Rule 113 (470 et seq.). See also Héctor Olásolo, *Unlawful Attacks in Combat Situations: From the ICTY's Case Law to the Rome Statute* (Nijhoff 2008) 155 et seq., 226 et seq., 256 et seq.; Helen Keller and Magdalena Forowicz, 'A tight-rope walk between legality and legitimacy: An analysis of the Israeli Supreme Court's judgment on targeted killing' (2008) 21 *Leiden JIL* 189, 213 et seq.; Gerd Hankel, *Das Tötungsverbot im Krieg: Eine Intervention* (Hamburger Edition 2011) 22 et seq.; Jason D Wright, '"Excessive" ambiguity: analysing and refining the proportionality standard' (2012) 94 *Intl Rev of the Red Cross* 819, 838 et seq., focusing especially on the ambiguous term 'excessive'.

[167] *Cf* Arts 22 and 23(e) Annex of the Hague Convention Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land (18 October 1907, entered into force 26 January 1910); Art. 35(1) and (2) AP I. See also Dinniss (n 10) 252–6. For possible war crimes see Art. 8(2)(b)(iii), (x), (xx), (xxv) and (e)(xi).

and severe damage to the environment'.[168] It defines indiscriminate attacks, going beyond Article 51(4) AP I, as attacks causing loss of civilian life and damage to civilian objects which is 'excessive in relation to the concrete and direct military advantage anticipated'.[169] Thus, an attack producing so-called collateral damage is not unlawful per se but only if the damage is excessive with regard to the military advantage.

The principle also applies to cyber attacks causing excessive collateral damage,[170] possibly amounting to 'superfluous injury or unnecessary suffering',[171] either during transit using civilian infrastructure or through the attack itself.[172] It offers, for the time being, a better protection than the static, less flexible principle of distinction.[173] Indeed, if one follows the strict view that any potential military use of a civilian object turns this object into a military objective the respective object would be a lawful target and only the proportionality excessive standard would provide for possible limits of cyber attacks. Take for example the case of a per se civilian cyber infrastructure like the electricity network of a major city which is only used to a limited extent for military purposes but for this reason would be considered dual-use and thus a lawful target. A cyber attack on such an infrastructure would probably have a serious civilian impact in cutting off all households and other civilian sites from the electricity supply. This 'collateral' civilian harm or damage, while not contravening the principle of distinction, would have to be balanced against the anticipated military advantage.[174]

Of course, the proportionality test would only be able to counter the adverse effects of the strict reading of the principle of distinction if the collateral or incidental damage brought about by the per se lawful cyber attack, i.e., 'loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof',[175] would be interpreted broadly.[176] Thus, collateral damage should encompass both direct and indirect effects of cyber attacks, i.e., the 'immediate, first order consequences' of the attack and 'the delayed and/or displaced second-, third- and higher-order consequences … created through intermediate events or mechanisms'.[177] In particular, as to incidental 'damage to civilian objects' a broad and dynamic interpretation is called for, including a mere loss of functionality of an attacked civilian object in the proportionality equation.[178] For the excessive evaluation one must try to determine as precisely as possible the adverse effects of a cyber attack on civilian cyber activities and relate them to

---

[168] Art. 35(3) AP I; see also Art. 55 AP I (in relation to protected objects) and Boothby (n 22) 394. For a possible war crime see Art. 8(2)(b)(iv).

[169] Art. 51(5)(b) and 57(2)(a) (iii) and (b) AP I. For a possible war crime see Art. 8(2)(b)(iv).

[170] Tallinn Manual 2.0 (n 6) Rule 113 (470): 'A cyber attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated is prohibited.'; see also Geiß and Lahmann (n 149) 395.

[171] Boothby (n 22) 391–2.

[172] Tallinn Manual 2.0 (n 6) Rule 113 (471).

[173] Geiß and Lahmann (n 149) 395–8, 398; see also Dervan (n 150) 389.

[174] See also Tallinn Manual 2.0 (n 6) Rule 113 (471) with the example of an attack on the GPS.

[175] *Cf* Art. 51(5)(b) and 57(2)(a) (iii) and (b) AP I as well as Tallinn Manual 2.0, ibid., Rule 113 (470).

[176] Geiß and Lahmann (n 149) 396–7.

[177] Tallinn Manual 2.0 (n 6) Rule 113 (472); see also ibid, 396; Droege (n 9) 572–3; Boothby (n 22) 390, 395, 397–8, 401.

[178] In this vein Geiß and Lahmann (n 149) 397–8; Geiss (n 66) 644–5. The Tallinn Manual experts also agreed that a 'deprivation of functionality' may in certain circumstances be included albeit explicitly excluding '*de minimis* damage' (n 6) Rule 113 (472) and Rule 92 (416).

the military advantage anticipated: 'The question is whether the harm that may be expected is excessive relative to the anticipated military advantage given the circumstances prevailing at the time'.[179]

The military advantage is to be determined equally precise ('concrete and direct'),[180] taking into account the attack as a whole[181] and prospectively ('anticipated'),[182] i.e., the respective commander has, on the one hand, a 'fairly broad margin of judgment',[183] also with regard to the possible collateral damage, but, on the other hand, faces a reasonableness test, i.e., his judgment must withstand a reasonableness analysis taking the 'reasonably well-informed person in the circumstances of the actual perpetrator' as the relevant standard.[184] Of course, the uncertainty of the indirect second, third etc. order effects of cyber attacks makes it – notwithstanding the above-mentioned technical possibility to limit their effects[185] – very difficult, for a commander to correctly anticipate the consequences of the attack.[186] It remains controversial, as in traditional IHL, whether a particularly great military advantage may outplay particularly serious or extensive damage, i.e., if a certain degree of damage may pose absolute limits to the proportionality equation.[187]

(iii) Principle of precaution

The overall objective of this principle is to minimize civilian harm to the greatest extent possible, regardless of any proportionality consideration as under the just discussed principle of proportionality. The principle has two limbs, i.e., it refers to precautions in attack (Art. 57 AP I) and precautions against the effects of attacks (Art. 58 AP I).[188] The failure to take such precautions may convert an otherwise permissible attack on a protected person or object into a war crime.

As to precautions in attack, Article 57(2) AP I lists a series of *active measures* to be taken by the conflict parties to spare civilians and civilian objects. In the cyber context, 'constant care' must be taken,[189] targets must be verified,[190] potential incidental effects limited to the greatest extent possible[191] and advance warnings given if cyber attacks may affect the civilian

---

[179] Tallinn Manual 2.0, ibid., Rule 113 (473); see also Boothby (n 22) 392.

[180] Tallinn Manual 2.0, ibid., Rule 113 (474), 'advantage … substantial and relatively close', referring to ICRC, Commentary AP, [2209].

[181] *Cf* ibid., Rule 113 (474).

[182] Ibid., Rule 113 (474), 'assessment of the reasonableness of the determination at the time of the attack … not to be applied with the benefit of hindsight'.

[183] Ibid., Rule 113 (475) referring to ICRC, Commentary AP, para 2210.

[184] *Prosecutor v Galic* (Judgment) IT-98-29-T (5 December 2003) para. 58; also *Prosecutor v Gotovina and Markač* (Judgment) IT-06-90-A (16 November 2012) para. 43; see also Tallinn Manual 2.0, ibid., Rule 113 (475) and Beck (n 113) 167, military advantage 'clear and obvious' to the attacker.

[185] See above n 153 with main text.

[186] On the uncertainty re the consequences see also Hathaway and others (n 4) 851; Dinniss (n 10) 207–8.

[187] In this vein Pilloud and others (n 135) [1980]; contra Tallinn Manual 2.0 (n 6) Rule 113 (473).

[188] See on its customary law status ICRC Study I (n 125), Rules 15–24.; see also Droege (n 9) 573 et seq.; from a US perspective see Wright (n 166) 830–2.

[189] Tallinn Manual 2.0 (n 6) Rule 114 (476).

[190] Ibid., Rule 115; stressing this as the main problem Beck (n 113) 170–71; see also Dinniss (n 10) 211–12.

[191] Ibid., Rule 116 (479–80), 'choice of means and methods of warfare … with a view to avoiding, and in any event to minimizing, incidental injury to civilians', and Rule 118 (481), choice of targets with

population.[192] The verification and limitation obligations may entail, for example, that the adversary's cyber network is mapped before the attack and the attack, as far as possible, limited to its military components.[193] Going beyond that one may even require that this limited attack is so designed as to avoid any incidental (collateral) effects with a view to the civilian cyber infrastructure.[194] All this requires technical expertise.[195] It is controversial, however, how far precautionary obligations go. While the normal standard is 'feasibility',[196] i.e., to do the 'practicable or practically possible, taking into account all circumstances',[197] in the case of military operations at sea or in the air 'reasonable precautions' suffice (Art. 57(4) AP I), i.e., less than feasibility is required.[198] Thus, in the example of a warship attacked by way of a cyber operation, two approaches exist: a strict view would require the mapping of the entire cyber infrastructure of this warship to be able to anticipate the (incidental) effects of the attack; a more liberal view contends that such a mapping would not be reasonable since the operation focuses on a target beyond land territory.[199]

As to the *passive* precautionary obligation to 'remove' civilian objects from military objectives (Art. 58(a) AP I) the interconnectivity problem already mentioned above makes this obligation in cyberspace difficult to fulfil: if the civilian and military infrastructure is intimately connected or – even worse – the cyberspace is a classical dual-use structure it is practically impossible to comply with this obligation, i.e., it is not 'feasible'[200] in the cyber context.[201] Article 58(c) AP I requires 'other necessary precautions' but they are, of course, also predicated upon the practical possibilities ('to the maximum extent feasible').[202] Thus, Article 58(c) is a 'catch-all' provision[203] trying to ensure protection of the civilian cyber infrastructure by other means than strict separation, i.e., 'to ensure a continuing cyber functionality' with regard to critical civilian infrastructure, for example by providing backups for power grids.[204]

---

a view 'to cause the least danger to civilian lives and to civilian objects'. See as primary norm Art. 57(3) AP I; on this provision Dinniss (n 10) 216–7.

[192] Ibid., Rule 120 (484).

[193] Droege (n 9) 573–4.

[194] See Tallinn Manual 2.0 (n 6) Rule 116 (480–81) with the example of inserting malware in a closed military network in a way to minimize collateral damage (mn. 6).

[195] Droege (n 9) 574; Tallinn Manual 2.0 (n 6) Rule 116 (480).

[196] Ibid., Rule 114 (477); see also Art. 58 AP I, 'to the maximum extent feasible' and Dinniss (n 10) 211.

[197] *Cf* Tallinn Manual 2.0, Ibid., Rule 114 (477) with further references in n 1157.

[198] Pilloud and others (n 135) 2230, 'all reasonable precautions must be taken, which is undoubtedly slightly different from and a little less far-reaching than the expression take all feasible precautions'.

[199] Tallinn Manual (n 17) 165 according to which the majority of the experts took the more liberal view (the Tallinn Manual 2.0 (n 6) no longer contain this quote); see also Dinniss (n 10) 217–19.

[200] Art. 58 AP I: 'to the maximum extent feasible'.

[201] *Cf* Zhixiong Huang and Yaohui Ying, 'The Application of the Principle of Distinction in the Cyber Context: A Chinese Perspective' (2021) 102 *Intl Rev of the Red Cross* 356 et seq.; Geiß and Lahmann (n 149) 392–4 therefore concluding that a segregation obligation cannot be deduced from this provision; in the same vein Droege (n 9) 575, 'hardly realistic'.

[202] See also Tallinn Manual 2.0 (n 6) Rule 121 (487 et seq.); with discussion of practical limitations ('feasibility').

[203] Ibid., 488.

[204] Geiß and Lahmann (n 149) 395; in a similar vein Droege (n 9) 576.

3. CYBER ATTACKS AND THE CRIME OF AGGRESSION[205]

Some authors contend that waging a cyber attack could constitute a breach of *ius ad bellum* and therefore lead to criminal liability for the crime aggression under Article 8*bis*(1) ICC Statute.[206] This view is, of course, predicated on the assumption that the respective cyber attack is carried out by a State since Article 8*bis* does not encompass the conduct of non-State actors.[207] In any case, it is difficult to envisage a cyber attack that falls under Article 8*bis.* While such an attack may in exceptional circumstances amount to an 'act of aggression' within the meaning of Article 8*bis*(2) lit.(d) ICC Statute, it will hardly amount to 'a manifest violation' of the UN Charter as required by Article 8*bis*(1) ICC Statute.[208] In addition, pursuant to the so-called *leadership clause*, criminal responsibility only arises with regard to 'a person in a position effectively to exercise control over or to direct the political or military action of a State' (Art. 8*bis*(1)). This means that the persons effectively carrying out a cyber attack would not be criminally liable under Article 8*bis* but, at best, their superiors, if they belong to the leadership level and can be held responsible for the acts of the actual 'cyber warriors'.

(a) 'Act of Aggression' Pursuant to Article 8bis (2) lit.(a)–(g) ICC Statute?

Paragraph 2 of Article 8*bis* ICC Statute requires a two-step analysis. First, it is to be examined whether a cyber attack would fall under one of the listed acts of aggression. Secondly, if this is not the case, the question arises whether the list of paragraph 2 is exhaustive or not.

(i) Listed acts in Article 8bis (2) ICC Statute

The listed acts in paragraph 2 are predicated on a 'use of armed force' as explicitly required at the beginning of this paragraph.[209] Pursuant to the *travaux préparatoires* the term 'armed force' is to be understood in a narrow sense referring to the employment of kinetic force by way of traditional weapons.[210] While a broader understanding was suggested during the nego-

---

[205] See also Roscini (Ch 14 of this Handbook).

[206] This position is represented by Johnatan Ophardt, 'Cyber warfare and the crime of aggression: The need for individual accountability on tomorrow's battlefield' (2010) 3 *Duke Law and Technology Rev* 3, 35; Noah Weisbord, 'Conceptualizing aggression' (2009) 20 *Duke Journal of Comparative and Intl L* 1 [Weisbord, Conceptualizing aggression]; Noah Weisbord, 'Judging aggression' (2011) 50 *Columbia J of Transnational* L 82 [Weisbord, Judging aggression]; Weissbrodt (n 4) 369; in a similar vein Chance Cammack, 'The Stuxnet worm and potential prosecution by the International Criminal Court under the newly defined crime of aggression' (2010) 20 *Tulane J of Intl & Comparative Law* 303.

[207] Crit. Ambos (n 26) 203–4.

[208] Conc. *Chaumette* (n 24) 9; thereto also Roscini (n 24) 251–2, arguing that 'the scale of the effects might not be significant or known enough, or attribution might not be clear' and that there is 'still debate on if and when a cyber attack is a use of armed force (and a fortiori an act of aggression) and thus falls under the scope of the jus ad bellum provisions of the Charter'. See also Carrie McDougall, *The Crime of Aggression under the Rome Statute of the ICC* (CUP 2013) 111, who sees a violation of Art. 2(4) UN Charter at least in the case of kinetic damage.

[209] This corresponds rather to 'armed attack' within the meaning of Art. 51 UN Charter than the broader 'use of force' within the meaning of Art. 2(4) UN Charter (for a comparison see Melzer (n 9) 11–2).

[210] *Cf* Matthew Gillett, 'The anatomy of an international crime: Aggression at the ICC' (2013) 13 *Intl Crim L Rev* 829, 838, explicitly excluding 'cyber warfare'.

tiations, including the inclusion of cyber attacks in paragraph 2,[211] it was finally rejected to avoid affecting 'the political or economic stability or exercise of the right to self-determination or violate the security, defence or territorial integrity of one or more States'.[212] Thus, while the negotiators apparently preferred a narrow understanding excluding cyber attacks at the outset, a broader approach could be defended on the basis of the effects-based approach applied above with regard to war crimes. Indeed, as rightly argued by one of the leading negotiators, a 'contemporary interpretation of the term armed force could, under some circumstances, include the use of computer networks as weapons'.[213]

The general understanding of the relevant provisions of the UN Charter, i.e., Article 2(4) referring to 'use of force' and Article 51 referring to an 'armed attack',[214] as only encompassing military, but not political or economic sanctions,[215] does not contradict this broader approach assuming that a cyber attack may, under certain circumstances, amount to a military attack. To qualify a cyber attack in that regard a set of factors has been proposed.[216] It is of course questionable if such a high number of (partly overlapping) factors contributes to legal certainty.[217] Ultimately, the severity of the attack seems to remain the decisive criterion.[218]

---

[211] *Cf* Stefan Barriga, 'Against the odds: The results of the Special Working Group on the Crime of Aggression' in Stefan Barriga, Wolfgang Danspeckgruber and Christian Wenawesser (eds), *The Princeton Process on the Crime of Aggression – Materials of the Special Working Group on the Crime of Aggression* (Lynne Rienner Publishers 2003–2009) 10, 'Suggestions were made to include non-conventional means of aggression beyond the use of armed force, such as cyber-attacks or economic embargoes'.

[212] *Cf* SWGCA, June 2008 Report (June 2008), in Assembly of States Parties to the Rome Statute of the International Criminal Court, Official Records, Resumed 6th sess (June 2008) ICC-ASP/6/20/Add.1, Annex II, para 35 https://asp.icc-cpi.int/iccdocs/asp_docs/ICC-ASP-6-20-Add.1%20English.pdf accessed 6 Oct. 2021. See also Barriga (n 211) 10, 'there was no desire to open the proverbial can of worms, and the great majority of delegations considered the limitation to the use of armed force as appropriate for the purpose of individual criminal justice'.

[213] Barriga (n 211) 10, fn. 44.

[214] For a thorough analysis and generally strict reading Dinniss (n 10) 37 et seq., 75 et seq.

[215] Generally, Albrecht Randelzhofer and Oliver Doerr, 'Article 2 4' in Bruno Simma and others (eds) *The Charter of the United Nations - A Commentary* (Vol. 1, OUP 2012) mn. 16–20; see in our context: Michael N Schmitt, 'Computer network attack and the use of force in international law: Thoughts on a normative framework' (1999) 37 *Columbia J of Transnational L* 885, 905–8; Daniel B Silver, 'Computer network attack as a use of force under Article 2(4) of the UN Charter' (2002) 76 *Intl L Studies* 73, 80 et seq.; Hathaway and others (n 4) 842; Weissbrodt (n 4) 358–60; Goldsmith (n 13) 133; see on the different scholarly approaches Dinniss (n 10) 58 et seq.

[216] Schmitt proposes with regard to the Art. 2(4) threshold a seven-factor test (Michael N Schmitt, 'Cyber operations and the jus ad bellum revisited' (2011) 56 *Villanova L Rev* 569, 576–7) which in the Tallinn Manual 2.0 (n 6) Rule 69 (334-6) is turned into an eight-factor test including severity, immediacy, directness, invasiveness, measurability of effects, military character, State involvement, presumptive legitimacy.

[217] See also Kessler and Werner (n 6) 808–9, arguing that this 'stamps the uncertainties surrounding the scope of the prohibition in the context of cyber attacks'.

[218] *Cf* Silver (n 215) 90 et seq. This is also stressed by the Tallinn Manual 2.0 (n 6) Rule 69 (334), pointing out that '[S]everity is the most significant factor in the analysis'. See also Melzer (n 9) 6 et seq.; Marco Benatar, 'The use of cyber force: Need for legal justification?' (2009) 11 *Goettingen J of Intl L* 376, 389 et seq.; Matthew C Waxman, 'Cyber attacks and the use of force' (2011) 36 *YJIL* 421, 432 et seq.; Michael Gervais, 'Cyber attack and the laws of war' (2012) 30 *Berkeley J of Intl* L 525, 539 et seq.; Dinniss (n 10) 63–5.

As to the listed acts *stricto sensu* only lit.(a), (b) and (d) can possibly be fulfilled by a cyber attack. While *lit.(a)* is less debated in this context at least one author considers that a computer can be an instrument for carrying out an 'attack of the territory of another state' when the 'use of force' has the necessary intensity and effects the territory.[219] *Lit.(b)* requires, in its second alternative, the 'use of any weapons' against State territory. If one defines 'weapons' in a traditional sense, as is indeed suggested by the requirement that it be directed 'against the territory of another State', the typical tools to carry out a cyber attack (e.g., by way of computer worms or viruses) would not be covered. Such a narrow interpretation would however go against the more flexible approach of the ICJ in the *Nuclear Weapons* opinion quoted above[220] and there is no convincing reason to exclude a cyber attack from the provision if it causes, in line with the effects approach,[221] the same or a similar damage as a conventional weapon.[222] Indeed, during the ICC negotiations on the aggression definition it was confirmed that the term 'weapons' is not limited to those which are described as conventional.[223] It is therefore argued by one of the leading negotiators that the word 'weapon' should be interpreted 'in conformity with the general definition of "armed force"'.[224] In addition, in the cyber context it has been suggested to define 'cyber weapons' as the 'means of cyber warfare'.[225] In sum, a cyber attack can be understood as 'the use of any weapon' in the sense of lit.(b).[226]

In any case, *lit.(d)*, requiring an 'attack by the armed forces' allows for a more liberal interpretation, encompassing cyber attacks carried out by members of the armed forces against the listed forces of another State. Indeed, a cyber attack on a developed country, which relies heavily on computer networks to operate its infrastructure (e.g., traffic control, water supply and the electrical grid) and its armed forces (e.g., air defence systems, modern fighter jets, drones or communications equipment) could lead to a partial or complete inoperability of the respective system. Indeed, in terms of the outcome, it does not matter whether national armed forces are inoperable due to strikes by 'conventional' armed force or due to a cyber attack.[227]

---

[219] Claus Kreß, 'The state conduct element' in Claus Kreß and Stefan Barriga (eds), *The Crime of Aggression: A Commentary* (Vol. 1, CUP 2017) 439.

[220] Above n 38 and main text.

[221] Above n 40 and main text.

[222] *Cf* Cammack (n 206) 322–3, arguing that 'many objectives for which armed force was used in the past are now being realized through nonmilitary, nonforceful pressures'; with regard to the Stuxnet attack against Iran he argues that according to subpara (b) 'the allowance of any weapons used against a territory will qualify' focusing on 'the damage or destruction caused'.

[223] Special Committee on the Question of Defining Aggression, *Official Records of the General Assembly*, 29th Session, Supplement No. 19, A/9619 and Corr. 1, para. 20, as quoted in Kreß (n 219) 442 fn. 146.

[224] Kreß, ibid., 442–3, noting that 'the presence of the armed forces of the aggressor state on the territory of the victim state' is not required.

[225] Tallinn Manual 2.0 (n 6) Rule 103 (452–3).

[226] Kreß (n 219) 443.

[227] The only difference is a higher probability of casualties in cases of conventional attacks (although a cyber-attack may also lead to fatalities, e.g., when it causes the total failure of a fighter jet's computer network in flight).

(ii) Is the list in Article 8bis (2) ICC Statute exhaustive?

As to the second question, i.e., whether the list is exhaustive, it has been argued elsewhere that this is the case.[228] Of course, the issue has been controversial during the negotiations[229] and there are views – sometimes invoking Article 4 of Resolution 3314[230] – which argue in favor of an open[231] or at least semi-open list including acts of the same nature (*eiusdem generis)*.[232] However, such a liberal interpretation does not sit well with the requirements of foreseeability and certainty demanded by the principle of legality (*nullum crimen sine lege*), as embodied in Articles 22–24 ICC Statute. Accordingly, criminal responsibility cannot be established *ex post facto* and the definitions of crimes must be strictly and precisely construed (*leges stricta* and *certa*).[233] If the drafters had wanted to apply the *eiusdem generis* doctrine, they could have adopted Article 4 of Res. 3314 or included a respective paragraph similar to the one in Article 7(1)(k) ICC Statute. Yet, they have not even given the UN Security Council – contrary to Article 4 of Res. 3314 – the right to extend or amend the list of Article 8*bis*(2) if it sees fit.[234]

---

[228] Ambos (n 26) 202. For the same view Gerhard Kemp, *Individual Criminal Liability for the International Crime of Aggression* (Intersentia 2010) 236; Helmut Satzger, *International and European Criminal Law*, (2nd edn C.H. Beck 2018) 322; Schmalenbach, 'Das Verbrechen der Aggression vor dem Internationalen Strafgerichtshof: Ein politischer Erfolg mit rechtlichen Untiefen' (2010) 65 *Juristenzeitung* 745, 748; Strapatsas, 'Aggression' in Schabas and Bernaz (eds), *The Routledge Handbook of International Criminal Law* (Routledge 2011) 155, 160; leaving it open Andreas Paulus, 'Second thoughts on the crime of aggression' (2009) 20 *EJIL* 1117, 1120, 'it remains open whether the list is meant to be exhaustive'.

[229] Special Working Group on the Crime of Aggression, 'June 2008 Report' (June 2008) ICC-ASP/6/20/Add. 1, Annex II, printed in: Barriga and Kreß (eds), *The Travaux Préparatoires of the Crime of Aggression* (CUP 2012) 602–14, 608; *cf* Robert Heinsch, 'The crime of aggression after Kampala: Success or burden for the future?' (2010) 2 *Goettingen J of Intl L* 713, 723–4.

[230] UNGA Res 3314 (14 December 1974) A/RES/3314, Art. 4, explicitly declaring that the list is not exhaustive and authorizing the Security Council to expand it.

[231] Andreas Zimmermann and Elisa Freiburg-Braun, 'Art. 8*bis* ICC-Statute' in Kai Ambos (ed), *Rome Statute of the ICC: A Commentary* (Beck 2022) mn. 157, but stressing that 'any other acts should be interpreted narrowly and must equate the character of the acts listed'; Gillett (n 210) 844-5; Christoph Safferling, *Internationales Strafrecht* (Springer 2011), mn. 183; in favour for an even broader and hardly plausible interpretation see Kevin Miller, 'The Kampala Compromise and cyberattacks: Can there be an international crime of cyber-aggression?' (2014) 23 *S Cal Interdisc L J* 217, 231 et seq.

[232] Roger S Clark, 'Negotiating provisions defining the crime of aggression, its elements and the conditions for ICC exercise of jurisdiction over it' (2009) 20 *EJIL* 1103, 1105; Roger S Clark, 'Amendments to the Rome Statute of the International Criminal Court considered at the first Review Conference on the Court, Kampala, 31 May–11 June 2010' (2010) 2 *Goettingen J of Intl L* 689, 696; more ambiguously Claus Kreß, 'Time for decision: Some thoughts on the immediate future of the crime of aggression: A reply to Andreas Paulus' (2009) 20 *EJIL* 1129, 1137, ''semi-open' at best […]'; Drew Kostic, 'Whose crime is it anyway? The International Criminal Court and the Crime of Aggression' (2011) 22 *Duke J of Comparative and Intl L* 109, 129–130; Ophardt (n 206) 66; see also Heinsch (n 229) 713, 723–6; Weisbord, Conceptualizing aggression (n 206) 40.

[233] On the *nullum crimen* principle see Ambos (n 25), 88–93. See also Barriga (n 211) 12; ibid., 'Negotiating the Amendments' in Barriga and Kreß (n 229) 30–31.

[234] Schmalenbach (n 228) 747–8; similar: Werle and Jeßberger (n 20) mn. 1607 et seq.; different: Weisbord, Conceptualizing Aggression (n 206) 40.

(b) Manifest Violation of the UN Charter (Article 8bis(1) ICC Statute)?

The threshold clause of Article 8*bis*(1) requires an 'act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations'. It expresses the qualitative difference between an 'act' of aggression which entails collective responsibility and a 'crime' of aggression which entails individual (criminal) responsibility.[235] Its purpose is to exclude minor incidents (e.g., border skirmishes) or legally controversial cases (e.g., a humanitarian intervention) from criminalization.[236] Thus, for example, the 2003 US-led invasion in Iraq, albeit considered by most international lawyers as an unlawful *act* of aggression,[237] might not have amounted to a *crime* of aggression due to the absence of a 'manifest' – i.e., from an objective perspective quantitatively and qualitatively serious[238] – 'violation' of the UN Charter in light of the fact that a respectable scholarly view existed according to which the invasion was justified, especially on the basis of Security Council Resolution 678 of 29 November 1990.[239] As for cyber attacks this means that it is difficult to envisage an attack which would be large and grave enough to amount to a manifest violation of the Charter. Indeed, as discussed in the previous section, it is even disputed whether cyber attacks constitute a simple violation of the Charter's prohibition of the use of force (Art. 2(4)) in the first place, especially because the effects approach cannot be employed without more.

According to the Tallinn Manual, a cyber operation constitutes a use of force 'when its scale and effects are comparable to non-cyber operations rising to the level of a use of force'.[240] The 'scale and effects' depend, in turn, on a series of factors to be taken into account.[241] What clearly seems to follow from that is that a cyber operation 'resulting in damage, destruction, injury, or death is highly likely to be considered a use of force',[242] i.e., more than mere economic or political coercion is required.[243] Thus, if one defines a cyber attack as causing death, injury or severe destruction to objects it amounts to a use of force. However, it this attack further constitutes a manifest violation of the Charter is an open question and depends on the specific circumstances of the case.

---

[235] *Cf* Ambos (n 26) 199; crit. Of the distinction Ilich F Corredor*, El Crimen de Agresión en Derecho Penal Internacional* (Universidad del Rosario 2012) 88–9.

[236] See SWGCA, 'June 2005 Report' (June 2005) ICC-ASP/4/32, Discussion Paper 3, No. 3, reprinted in Barriga, Danspeckgruber and Wenaweser (n 211) 197; see also Barriga (n 211) 8; Barriga and Kreß (n 229) 29; Roger Clark, 'Alleged aggression in Utopia' in William Schabas, Yvonne McDermot and Niamh Hayes (eds), *The Ashgate Research Companion to International Criminal Law* (Ashgate 2013) 66.

[237] See Claus Kreß, 'Strafrecht und Angriffskrieg im Licht des "Falles Irak"' (2003) 115 *Zeitschrift für die Gesamte Strafrechtswissenschaft* 294, 313 et seq.

[238] The term is certainly ambiguous, *cf* Paulus (n 228) 1121; for an – not entirely convincing – explanation see Kreß (n 232) 1137 et seq. The objective perspective is determined by Element 3 of the Introduction to the Elements of Crimes to Art. 8*bis* ICC Statute.

[239] Kreß (n 237) 331; critically Paulus (n 228) 1123.

[240] Tallinn Manual 2.0 (n 6) Rule 69 (330).

[241] *Cf* ibid., Rule 69 (333 et seq.), severity, immediacy, directness, invasiveness, measurability of effects, military character, State involvement and presumptive legality.

[242] Tallinn Manual (n 17) Rule 10 (48); the Tallinn Manual 2.0 (n 6) does no longer contain this quote but, of course, still follows the effects approach.

[243] See also Tallinn Manual 2.0, ibid., Rule 69 (331).

4. CYBER ATTACKS AND CRIMES AGAINST HUMANITY

Crimes against humanity require that the actual underlying conduct, for example, murder, torture, rape or imprisonment, has been 'committed as part of a widespread or systematic attack directed against any civilian population' (Art. 7(1) ICC Statute). This is the context element of crimes against humanity. While the requirement of an attack 'against any civilian population' has its origin in the laws of war and thus largely draws, pursuant to the traditional view,[244] on the distinction between civilians and combatants already discussed above with regard to war crimes, the 'widespread or systematic attack' is the peculiar feature of crimes against humanity. Insofar, the wording of Article 7(2)(a) ICC Statute implies that this requirement has to be understood qualitatively, i.e., the 'attack' must always – notwithstanding its predominantly 'widespread' or 'systematic' character – be based on ('pursuant to or in furtherance of') a certain policy.[245]

As to cyber attacks this means that they must, first of all, be carried out pursuant to a certain policy and, further, be widespread or systematic. The policy requirement presupposes that such attacks are planned, organized, coordinated or at least tolerated by a State or organization within the meaning of Article 7(2)(a) ICC Statute. If this is the case the attack would normally also be qualified as 'systematic'.[246] While a loosely organized group of hackers acting autonomously would not meet the organizational requirement, organized armed groups within the meaning of IHL that take recourse to methods of cyber warfare certainly would.[247] If, further, the cyber attacks carried out by a State or a sufficiently organized group caused severe and extensive damage, in the sense of the examples given above, the attack could, arguably, also be qualified as 'widespread'. Such widespread or systematic cyber attacks may, finally, result in the killing or extermination of civilian populations or even in one of the other underlying acts of Article 7 ICC Statute. Of course, ultimately, the fulfilment of the elements of a crime against humanity will depend on the circumstances of the concrete case.

5. CONCLUSIONS

Individual criminal liability for cyber attacks may rather arise in connection with war crimes than for a crime of aggression. Waging a 'cyber war' under violation of the *ius ad bellum* will rarely lead to criminal liability for aggression under Article 8*bis* ICC Statute, since it is rather difficult to envisage that a cyber attack amounts to an act of aggression within the meaning of Article 8*bis*(2) ICC Statute, let alone to a manifest violation within the meaning of Article 8*bis*(1) ICC Statute.

IHL applies to cyber attacks without further ado if such attacks are part of an ongoing conflict. In the absence of such a conflict, the cyber attacks must themselves be serious enough to pass the armed conflict threshold. This is the case if, following the effects approach, a cyber attack causes considerable human and other damage, going beyond mere sporadic and isolated incidents causing only inconvenience or the temporary shutdown of computer systems. Cyber

---

[244] For a more liberal interpretation of this element however Ambos (n 26) 63 et seq.
[245] *Cf* ibid., 63, 67 et seq.
[246] *Cf* ibid., 59–61.
[247] On the respective dispute in the ICC's Kenya decision see ibid., 72 et seq.

attacks producing such effects also qualify as armed attacks within the meaning of Article 49(1) AP I. To qualify as a war crime a cyber attack must be linked to an ongoing armed conflict. Attribution is possible if the attacker can be identified and acts on behalf of a conflict party within the meaning of IHL, i.e., either a State (in an international armed conflict) or an organized armed group (in a non-international armed conflict). Cyber attacks of less organized groups of individuals which do not qualify themselves as a conflict party may be attributed to such a party pursuant to the rules of State responsibility or of the ICRC Interpretive Guidance.[248] For 'pure' civilian cyber participants the rules on the direct participation in hostilities apply.

As to the IHL principles governing the conduct of hostilities the principle of proportionality appears to have the greatest capacity to limit harm to civilians and civilian objects. In contrast, the principle of distinction is of little practical relevance given the high interconnectivity between military and civilian computer systems and the mostly dual use of cyber infrastructure. The principle of precaution also guides the conduct of cyber operations, but it is itself limited by feasibility or reasonability considerations. All in all, IHL seems to be sufficiently broad and flexible enough to accommodate the new developments with regard to cyber warfare.[249] However, as the effectiveness of the rules often depends on their broad or restrictive interpretation, 'more stringent rules' may prove necessary.[250]

Cyber attacks passing the armed conflict threshold may also constitute systematic or widespread attacks within the meaning of Article 7 ICC Statute. In any case, they must be carried out pursuant to a policy of a State or an organization within the meaning of Article 7(2)(a) ICC Statute.

---

[248] Supra n 75 et seq. and main text.
[249] In the same vein Dinniss (n 10) 28–9, 279.
[250] In the same vein Droege (n 9) 540, 578.

9. International investment law and arbitration in cyberspace

Eric De Brabandere

INTRODUCTION

Cybersecurity in international investment law and arbitration is a recent point of attention. Foreign investors, as any other businesses, are increasingly subjected to cyberattacks as part of the general rise of cyberattacks. Cyberattacks also have increased in terms of sophistication.[1]

In 2015, it was estimated that up to 50 per cent of small businesses had been victims of cyberattacks, and 60 per cent of those who suffered a significant cyberbreach went out of business within six months.[2] On average, one out of three businesses confronted with cyberattacks ended up paying a 'ransom' to the perpetrators.[3] The past years have witnessed several major cyberattacks on multinational enterprises, such as the well-reported 2010 attack on Google,[4] the attacks on Exxon Mobile that same year,[5] and also less reported attacks on companies such as the January 2020 large-scale ransomware attack on the Belgian company Picanol Group which resulted in a temporary halt of production capacity and hence important financial losses.[6]

Cyberattacks result in various forms of damage, such as information loss, business disruption, revenue losses and damage to equipment.[7] In general, it has been reported that businesses lose on average '0.8 percent of their market value in the seven days following news of an

[1] For a general discussion, see Scott J Shackelford and others, 'Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets Through Bilateral Investment Treaties' (2015) 52 *American Business Law Journal* 1, 7 *ff*.

[2] International Bar Association, 'Cybersecurity Guidelines' (2018) 4.

[3] Karsten Lemmens, 'Eén bedrijf op drie betaalt losgeld aan cybercriminelen', *De Standaard* (12 May 2020) www.standaard.be/cnt/dmf20200512_04955876 accessed 13 May 2020.

[4] Melanie Lee and Lucy Hornby, 'Google Attack puts Spotlight on China's "red" Hackers', *Reuters* (20 January 2010) www.reuters.com/article/us-google-china-hackers/google-attack-puts-spotlight-on-chinas-red-hackers-idUSTRE60J20820100120 accessed 30 April 2020.

[5] David Collins, 'Applying the Full Protection and Security Standard of International Investment Law to Digital Assets' (2011) 12 *Journal of World Investment and Trade* 225, 234.

[6] See 'Press Release: cyber attack', *PICANOL* (31 January 2020) www.picanol.be/news/press-release-cyber-attack-update-january-31-2020 accessed 30 April 2020.

[7] The Council of Economic Advisers, 'The Cost of Malicious Cyber Activity to the U.S. Economy' (February 2018) 7 www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf accessed 6 May 2020.

adverse cyber event'.[8] This in turn has resulted in average financial losses ranging from $2.7 million[9] to $498 million per adverse cyber event.[10]

The question of cybersecurity, and the role and responsibility of the host State in which the foreign investor has invested has thus gained prominence, although so far based on the current publicly available information, no claim on that ground seems to have been brought. First of all, States seem to increasingly rely on concerns relating to the digital economy, such as security and consumer protection, in order to take measures or adopt a certain conduct which in itself may be considered detrimental to foreign investors and constitute a breach of the State's investment treaty obligations. Secondly, investment claims by targeted foreign investors against the host State for failure to provide the necessary security cannot be excluded.

When analysing these issues from the perspective of international investment law and arbitration, and before turning to possible violations of investment protection standards by host States, one first will need to identify whether the 'digital assets', which are the subject of cybersecurity and targeted by cyberattacks qualify as 'investments'. Moreover, the question of the precise location of the assets will be determinative since investment treaties often provide for investments to have been made 'in the territory' of the host economy. A related question is whether entry requirements for foreign investors, that is the 'admission' and 'establishment' of foreign investors, which are sometimes, but not always, included in investment treaties may also present specific issues in relation to cybersecurity threats and concomitant security screening that may be organised by host States for foreign investment in digital assets.[11] Once it can be established that digital assets constitute an investment under the applicable legal instruments, the question then is whether international investment treaties can provide a basis for claims by foreign investors against host States for internationally wrongful acts caused to their digital assets.

In line with the general approach adopted in this Handbook, this chapter does not attempt to provide definitive answers to all issues potentially relevant to foreign investment in cyberspace. Rather, the objective is to map out possible connections between contemporary international investment law and arbitration and foreign investment in cyberspace.

In this chapter, I will first address the question of whether digital assets can qualify as 'investments', as defined both in international investment treaties and under the Convention on Settlement of Investment Disputes (ICSID Convention).[12] I will next address the related question of entry requirements for foreign investors and security screening operated by host States for investments in digital assets.[13] I will then turn to analysing possible claims by foreign investors against host States for breaches of their obligations, under applicable international investment treaties, in relation to cybersecurity. This will be done through an analysis of what

---

[8] Ibid., 8.

[9] PWC, '*Managing cyber risks in an interconnected world* – Key findings from The Global State of Information Security® Survey 2015' (30 September 2014) 10 www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf accessed 6 May 2020.

[10] Council of Economic Advisers (n 7) 8.

[11] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (OUP 2012) 88.

[12] Convention on the Settlement of Investment Disputes between States and Nationals of Other States (opened for signature 18 March 1965, entered into force 14 October 1966) 575 UNTS 159.

[13] Dolzer and Schreuer (n 11) 88.

I consider to be the two most relevant provisions regularly found in international investment treaties: fair and equitable treatment (FET) and (full) protection and security (FPS).

1. DIGITAL ASSETS AS AN 'INVESTMENT'

Digital assets, which can comprise websites, consumer and customer data and contracts,[14] and computer systems,[15] are broad categories which are difficult to define in abstract terms. The UNCTAD 2017 World Investment Report[16] however has classified most relevant multinational enterprises (MNEs) active in the 'digital economy' into two groups: the first are the so-called 'Digital MNEs', which are:

> characterized by the central role of the internet in their operating and delivery model. They include *purely digital players* (internet platforms and providers of digital solutions) that operate entirely in a digital environment and *mixed players* (e-commerce and digital content) that combine a prominent digital dimension with a physical one.[17]

These include businesses active in the following fields: internet platforms, digital solutions, e-commerce, and digital content.[18] The second group are so-called 'ICT MNEs', which 'provide the enabling infrastructure that makes the internet accessible to individuals and businesses. It includes IT companies selling hardware and software, as well as telecom firms'.[19] For ease of reference, I will hereafter refer to these forms of investments as composed of 'digital assets'.

Legally, digital assets are difficult to categorise, not only because they are mostly intangible by their very nature and constituted by a variety of distinct sub-components, but also because digital assets in and of themselves often do not often exist as stand-alone 'investments'. In other words, digital assets often form part of a broader (set of) investment(s). The question then is whether digital assets can be considered as 'investments' either in and of themselves or as part of a broader investment made by a foreign investor.

1.1 'Investment' under International Investment Treaties and ICSID Convention

In order to benefit from the protection of an international investment treaty, the digital assets invariably need to fall under the definition of 'investment' in that treaty either as such or as part of a larger investment. Moreover, in case disputes relating to the digital assets are brought

---

[14] On this, see Andrew D Mitchell, Tania Voon and Jarrod Hepburn, 'Taxing Tech: Risks of an Australian Digital Services Tax under International Economic Law' (2019) 20 *Melbourne Journal of International Law* 88, 115-8.

[15] See Julien Chaisse and Cristen Bauer, 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' (2019) 21 *Vanderbilt Journal of Entertainment & Technology Law* 549, 556 *ff.*

[16] UNCTAD, 'World Investment Report 2017 – Investment and the Digital Economy' (2017) UN Doc UNCTAD/WIR/2017 https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1782 accessed 28 April 2020.

[17] Ibid., 165.

[18] Ibid.

[19] Ibid.

to arbitration under the ICSID Convention, such assets need to be captured also by the notion of 'investment' as understood by Article 25 of the ICSID Convention which defines and delimits the jurisdiction of the ICSID.

The vast majority of investment treaties contain wide and broad definitions of what constitutes an 'investment'. The wide definitions usually present in investment treaties often are similarly structured and consequently follow a similar approach. Yet, and this is a point generally valid for the entire chapter, international investment treaties are not identical which means that most treaties, while containing similar definitions of 'investment', do leave room for nuance and hence any attempt at generalisation is hazardous for that reason only.

Nonetheless, it is safe to say that most treaties employ a so-called 'asset-based definition'.[20] The asset-based definition can stand by itself, that is, the term 'asset' is not defined. Any 'asset', then, can technically constitute an investment. An example of a broad 'stand-alone' asset-based definition is the 2006 Mexico-United Kingdom (UK) Bilateral Investment Treaty (BIT): '"investment" means an asset acquired in accordance with the laws and regulations of the Contracting Party in whose territory the investment is made (…)'.[21]

Other treaties contain a broad asset-based definition which adds substantive characteristics to investments, such as the 'commitment of capital or other resources, the expectation of gain or profit, or the assumption of risk'.[22]

Such clauses have usually been interpreted as attempts to 'distinguish investments from transactions of an ordinary, short-term character (e.g., the sale of a good or a service or a short-term financial transaction) in order to exclude the latter from the treaty' protection'.[23]

Sometimes,[24] the broad definition is followed by a non-exhaustive list of examples of forms investments can take with or without exclusions, or, less commonly, by an exhaustive list[25] of examples of forms investments can take. The 2006 Mexico-UK BIT provides an example of a non-exhaustive list.[26] While the level of detail of the list varies,[27] most lists can often be brought down to five categories: (1) movable and immovable property; (2) various interests in companies and enterprises such as shares; (3) claims or titles to money; (4) intellectual

---

[20] Jeswald W Salacuse, *The Law of Investment Treaties* (OUP 2015) 176. There are however exceptions. The Canada-Serbia 2014 Bilateral Investment Treaty for instance contains only a (rather broad) list of what constitutes an investment and has no broad asset-based definition. See Agreement between Canada and the Republic of Serbia for the Promotion and Protection of Investments (signed 1 September 2014, entered into force 27 April 2015) (Canada-Serbia BIT) Art 1.

[21] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United Mexican States for the Promotion and Reciprocal Protection of Investments (signed 12 May 2006, entered into force 25 July 2007) (Mexico-UK BIT) Art 1.

[22] Treaty between the Government of the United States of America and the Government of the Republic of Rwanda concerning the Encouragement and Reciprocal Protection of Investment (signed 19 February 2008, entered into force 1 January 2012) (US-Rwanda BIT) Art 1.

[23] Salacuse (n 20) 181.

[24] See e.g., Agreement between the Government of Sweden and the Government of the Socialist Federal Republic of Yugoslavia on the mutual protection of investments (signed 10 November 1978, entered into force 21 November 1979) (Serbia-Sweden BIT) Art 1.

[25] Canada-Serbia BIT (n 20) Art 1.

[26] Mexico-UK BIT (n 21) Art 1.

[27] Cf Agreement on encouragement and reciprocal protection of investments between the Kingdom of the Netherlands and the Federal Republic of Yugoslavia (signed 29 January 2002, entered into force 1 March 2004) (Netherlands-Serbia BIT) Art 1, with the Mexico-UK BIT cited in the previous note.

property rights; and (5) concessions or licences.[28] In any event, since more often than not these lists are merely examples of forms investments may take, tribunals have regularly confirmed that the broad asset-based definitions 'are designed to protect as wide a range of investment forms as possible'.[29]

Even when treaties include a broad asset-based definition, purely commercial transactions may be excluded from the scope of application of investment treaties. The Mexico-UK BIT mentioned above, for instance, clearly excludes purely commercial transactions, such as 'claims to money' if these are not part of or related to a form of investment which falls under the scope of application of the treaty.[30] Other treaties, however, contain generic references to 'claims to money, to other assets or to any performance having an economic value'[31] which has been interpreted as to broaden the definition of 'investment' beyond the traditional understanding of the term 'asset'.[32]

In defining what constitutes an 'investment' under a treaty, international investment treaties may add the requirement for the investment to be made in the territory of one of the contracting parties, in order for the investment to be 'international'. The 2006 Mexico-UK BIT mentioned above, for example, provides that the investment needs to be made in the territory of one of the States.[33] While the 'territoriality' question is relatively easy to answer in the case of tangible assets, which by their very nature are located somewhere, the location of intangible assets is more difficult to determine. In relation to financial instruments, the tribunal in *Fedax v Venezuela* decided that these can be considered to have been made in the territory of the host State if the available funds are used by or put at the disposal of the beneficiary State.[34] Also, while single operations may not have taken place in the territory of the host State, tribunals have looked at the question whether investments 'considered as a whole' are made in the territory of the host State.[35]

In relation to financial instruments, the tribunal in *Abaclat v Argentina* also accepted that 'the relevant criteria should be where and/or for the benefit of whom the funds are ultimately used'.[36] The decision however was taken only by a majority, and heavily criticised, including

---

[28] Salacuse (n 20) 177.

[29] Ibid., 180.

[30] Mexico-UK BIT (n 21) Art 1 (i)–(J).

[31] Netherlands-Serbia BIT (n 27) Art 1(a)(iii).

[32] Salacuse (n 20) 180.

[33] Mexico-UK BIT (n 21) Art 1. Other treaties include the requirement in provisions relating to the substantive protection standards contained in the treaty, such as the Albania-Serbia Bilateral Investment Treaty which extends protection to 'investments made by investors of one Party in the territory of the other Party': Agreement between the Federal Government of the Federal Republic of Yugoslavia and the Council of Ministers of the Republic of Albania on the reciprocal promotion and protection of investments (signed 26 November 2002, entered into force 14 May 2004) (Albania-Serbia BIT) Art III (1).

[34] *Fedax NV v The Republic of Venezuela*, ICSID Case No ARB/96/3, Decision of the Tribunal on Objections to Jurisdiction (11 July 1997) para 41. For a discussion, see Salacuse (n 20) 188 and Dolzer and Schreuer (n 11) 189.

[35] *SGS Société Générale de Surveillance SA v Republic of the Philippines*, ICSID Case No ARB/02/6, Decision of the Tribunal on Objections to Jurisdiction (29 January 2004) para 112.

[36] *Abaclat and Others v Argentine Republic*, ICSID Case No ARB/07/5 (formerly *Giovanna a Beccara and Others v The Argentine Republic*), Decision on Jurisdiction and Admissibility (4 August 2011) para 374.

on this particular point, by Arbitrator Georges Abi-Saab in his dissenting opinion who argued that 'a territorial link or nexus is inherent in the concept of "investment"'.[37]

Before looking at the implications of the preceding principles and practices for the question of whether digital assets could be categorised as 'investments', it is important to add that, in case of arbitration under the ICSID Convention, the 'investment' must not only be captured by the definition contained in the investment treaty, but also fall under the scope of Article 25 ICSID Convention. Article 25 ICSID extends the jurisdiction of the Centre to 'any legal dispute arising directly out of an investment' but fails to further define 'investment'. The lack of a clear definition of what constitutes 'investment' for the purposes of Article 25 ICSID has triggered a 'wide-ranging debate'[38] in scholarship and practice. I do not intend to engage in that debate here, but it is necessary to explain the two main theories or approaches on the question.

A first approach consists of considering that the notion of 'investment' under Article 25 ICSID has an objective meaning that is independent of the parties' understanding of the concept. Thus construed, 'investment' under Article 25 ICSID requires four features: a substantial commitment; a certain duration of performance; participation in the risks of the transaction; and a contribution to the development of the host State.[39] These criteria were set out by the tribunal in *Salini v. Morocco*[40] and have since then been referred to as the 'Salini criteria'.

A second approach consists of operating a 'renvoi' to the definition of investment agreed by the States in their investment treaty which contains the consent to arbitration, thus emphasising party autonomy in defining what constitutes an 'investment'.[41] This, it has been argued is in conformity with the drafting and negotiating history of ICSID.[42]

Tribunals essentially follow one or the other approach, or adopt a reasoning which combines both.[43] However, in general, and whichever the approach to the notion of 'investment' under the ICSID Convention, one-time purely commercial transactions usually are considered to fall outside the concept of 'investment', based on the fact the ordinary meaning or general understanding of 'investment', even in the case of a renvoi to the treaty definitions agreed by the parties, refers to transactions other than purely commercial transactions.[44]

1.2 Can Digital Assets Qualify as 'Investments'?

Based on the principles set out above, several issues arise when dealing with digital assets as 'investment' for the purpose of international investment law.

---

[37] Ibid., Dissenting Opinion to Decision on Jurisdiction and Admissibility by Georges Abi-Saab, para 74.

[38] Dolzer and Schreuer (n 11) 65.

[39] Ibid., 66.

[40] *Salini Costruttori SpA and Italstrade SpA v Kingdom of Morocco*, ICSID Case No ARB/00/4, Decision on Jurisdiction (23 July 2001) para 56.

[41] See for a discussion see Dolzer and Schreuer (n 11) 68–76. See also e.g., *Pantechniki SA Contractors & Engineers (Greece) v The Republic of Albania*, ICSID Case No ARB/07/21, Award (30 July 2009) paras 42 *ff*.

[42] See for a discussion see Dolzer and Schreuer (n 11) 68–76. See also e.g., *Pantechniki SA Contractors* (n 41) paras 42 *ff*.

[43] Dolzer and Schreuer (n 11) 69.

[44] Ibid., 75.

First of all, the broad asset-based definitions usually present in international investment treaties, extending the coverage of these treaties to all assets without any limitation might, because of their broad and non-exhaustive nature, be interpreted as to cover digital assets or businesses.[45] As put by UNCTAD, such definitions suggest 'that the term embraces everything of economic value, virtually without limitation'.[46] As a consequence, authors have argued that digital assets can, because of their intrinsic or extrinsic value, fall under the broad asset-based definitions.[47]

In addition to the broad asset-based definition, the list of forms investments may take, which some treaties also provide, can further confirm that digital assets cannot, merely because of their intangible nature, be excluded from the definition of 'protected investment',[48] especially if the list refers generically to 'intangible assets'. Article 1(g) of the Mexico-UK BIT, for example, mentions 'real estate or other property, tangible or intangible, including intellectual property rights, acquired in the expectation or used for the purpose of economic benefit or other business purposes'.[49]

Aside from the possibility of considering digital assets as 'investments' in and of themselves, a holistic approach to 'investment' may also lead to the conclusion that digital assets are 'covered investments'. Under a holistic approach, the individual elements of digital businesses are not viewed in isolation but assessed from the perspective of the 'unity of an investment operation'.[50] Individual components of investment operations, such as digital assets, may thus be considered as an 'investment' if they form part of a broader investment operation. Investment in the digital sector indeed usually implies other forms of investment, such as investment in infrastructure.[51] As noted by Nicholas Tsagourias in his chapter in this Handbook, 'cyberspace has three layers: a physical layer which consists of computers, integrated circuits, cables, communications infrastructure and the like; a second layer which consists of the software logic; and, finally, a third layer which consists of data packets and electronics'.[52]

However, one should keep in mind that certain treaties do contain more narrow definitions, and that investments need to be distinguished from 'transactions of an ordinary, short-term character (e.g., the sale of a good or a service or a short-term financial transaction) which may be excluded from the treaty's protection'.[53] This is the case notably for those treaties which add additional characteristics of investments to the broad asset-based definition.[54] Hence,

---

45 Chaisse and Bauer (n 15) 557–8.

46 UNCTAD, 'Series on Issues in International Investment Agreements: Scope and Definition' (2011) UN Doc UNCTAD/ITE/IIT/11(Vol. II) 18 https://unctad.org/en/pages/PublicationArchive.aspx?publicationid=341 accessed 30 April 2020.

47 Chaisse and Bauer (n 15) 559.

48 Ibid.

49 Mexico-UK BIT (n 21) Art 1.

50 Mitchell, Voon and Hepburn (n 14) 116. See also Christoph Schreuer and Ursula Kriebaum, 'At What Time Must Legitimate Expectations Exist?' in Jacques Werner and Arif H Ali (eds), *A Liber Amicorum: Thomas Wälde. Law Beyond Conventional Thought* (CMP Publishing 2009) 267. See also *Ceskoslovenska Obchodni Banka, AS v The Slovak Republic*, ICSID Case No ARB/97/4, Decision of the Tribunal on Objections to Jurisdiction (24 May 1999) para 72.

51 World Investment Report 2017 (n 16) 190 *ff*.

52 Tsagourias (Ch 1 of this Handbook).

53 Salacuse (n 20) 181.

54 US-Rwanda BIT (n 22) Art 1.

there remains a certain uncertainty and categorically positing that digital assets would always qualify as 'investment' under an investment treaty is difficult.

For the same reason, whether or not digital assets would fall under the Article 25 ICSID notion of 'investment' is difficult to establish with certainty, especially if a tribunal decides to adhere (even partly) to the 'Salini-criteria' which require a substantial commitment, a certain duration of performance, participation in the risks of the transaction, and a contribution to the development of the host State.[55] Here again, the main principle would be that single one-off commercial transactions of digital businesses would not be captured by the notion of 'investment' under the ICSID Convention, while transactions which have a long-term commitment and meet the other criteria would not necessarily be excluded.[56]

In respect of the territorial link, as noted by UNCTAD, '[b]ecause "investment" includes many intangible rights, the location of a particular asset may be difficult to identify'.[57] In general, factors such as location of, and possession and control over the digital assets will be important and determinant for the establishment of the territorial link between the digital assets and the host State.[58] In respect of the 'physical layer'[59] of digital businesses, the territorial nexus will be less difficult to ascertain, as will be the case for digital assets such as software which are contained on a physical device.[60] The most tricky part will be establishing the territorial link for purely intangible digital assets such as data. Based on the case-law discussed above, one can only conclude that the answer to this question is difficult also. If one accepts the approach to look at whether investments 'considered as a whole' are made in the territory of the host State,[61] hence at the investment operation as a whole of which digital assets form a part, the territorial nexus can be established to the extent of course that the entire investment operation is made in the territory of the host State. Looking at the digital assets as stand-alone or individual investment operations, one may need to look at 'where and/or for the benefit of whom' the assets are ultimately used.[62] The link 'to a specific economic enterprise or operation taking place in the territory of the Host State'[63] would then play a minor role. However, looking at the same question from the perspective of the dissent of Georges Abi-Saab in that case, in which he had argued that there should be a 'specific economic anchorage' in the host economy,[64] one could arrive at the opposite conclusion.[65]

---

[55] Dolzer and Schreuer (n 11) 66.

[56] Chaisse and Bauer (n 15) 562–3.

[57] UNCTAD, 'Series on Issues in International Investment Agreements: Scope and Definition' (2011) UN Doc UNCTAD/ITE/IIT/11(Vol. II) 45 https://unctad.org/en/pages/PublicationArchive.aspx?publicationid=341 accessed 30 April 2020.

[58] Chaisse and Bauer (n 15) 564.

[59] Tsagourias (Ch 1 of this Handbook).

[60] Chaisse and Bauer (n 15) 565.

[61] *SGS Société Générale de Surveillance SA* (n 35) para 112.

[62] *Abaclat and Others* (n 36) para 374.

[63] Ibid., para 375.

[64] Ibid., Dissenting Opinion to Decision on Jurisdiction and Admissibility by Georges Abi-Saab, para 108.

[65] A link here can also be made with the question of whether the State can exercise jurisdiction over the digital assets. See *in extenso* Tsagourias (Ch 1 of this Handbook) and Kohl (Ch 4 of this Handbook).

2. DIGITAL ASSETS, ENTRY REQUIREMENTS, AND SECURITY SCREENING

Before turning to the substantive protection standards in their application to digital investments, it is important to consider entry requirements for foreign investors, that is 'admission' and 'establishment' of foreign investment. 'Admission' refers to the entry of the investment as such, while 'establishment' of foreign investors refers to the 'conditions under which the investor is allowed to carry out its business during the period of the investment'.[66]

In relation to investment in the digital economy, admitting foreign investment, and authorising foreign investors to invest or establish themselves in the territory of a State may pose distinct problems. Notably, security concerns may affect the entry of investors to foreign markets. This is the case for investment in the defence industry, critical infrastructure and strategic economic sectors, which have typically been subjected to more profound scrutiny and screening by the host economy.[67] For several years, some States have toughened their security screening for foreign investment,[68] notably to assess possible security risks in relation to investment in the digital economy by foreign State-Owned Enterprises (SOEs).[69]

There are roughly two models of investment treaty provisions when it comes down to admission and establishment. In a first set of treaties typically concluded by European States or treaties concluded by other States but modelled on 'European' treaties, foreign investors are not granted a right of admission or establishment.[70] Admission or establishment is only possible in accordance with the host State's legislation.[71] Such investment treaties thus mostly provide for 'post-entry' treatment, and contain no commitments to admit foreign investors, or authorise establishment of foreign investors. Domestic law only regulates admission and may authorise differentiated treatment of foreign investors.

Under a second model, mostly followed by Canada and the United States, a limited right of admission is granted under the investment treaty.[72] The right of admission is limited, since it in fact extends national treatment (NT) and often also most-favoured nation treatment (MFN) to the establishment, acquisition or expansion of the investment.[73] In other words, a form of guarantee of non-discrimination in relation to the establishment, acquisition or expansion of the investment is provided. Most treaties which contain such admission rights also usually contain

---

[66] Dolzer and Schreuer (n 11) 88.

[67] UNCTAD, World Investment Report 2016 – Investor Nationality: Policy Challenges (2016) UN Doc UNCTAD/WIR/2016, 95 https://unctad.org/en/PublicationsLibrary/wir2016_en.pdf accessed 13 May 2020.

[68] Ibid., 94 *ff.*

[69] See generally Lu Wang, 'Chinese SOE Investments and the National Security Protection under IIAs' in Julien Chaisse, *China's International Investment Strategy: Bilateral, Regional, and Global Law and Policy* (OUP 2019) 67–86.

[70] Dolzer and Schreuer (n 11) 89.

[71] See e.g., Treaty between the Federal Republic of Germany and the Kingdom of Bahrain concerning the Encouragement and Reciprocal Protection of Investments (signed 5 February 2007, entered into force 27 May 2010) (Bahrain-Germany BIT) Art 2(1).

[72] Dolzer and Schreuer (n 11) 89.

[73] See e.g., 2012 Treaty between the Government of the United States of America and the Government of [Country] concerning the encouragement and reciprocal protection of investments (US Model BIT) Arts 3 and 4.

a list of sectors or activities to which the clauses on NT and MFN treatment do not apply.[74] These sectors are then listed in a 'positive list' – including all sectors that are 'open' to foreign investment, or a 'negative list' which contains only the exceptions to the general 'openness' of all sectors or activities. 'Closed' sectors in investment treaties may include, for example, banking, insurance, securities, and 'one-way satellite transmissions of direct-to-home (DTH) and direct broadcast satellite (DBS) television services and of digital audio services'.[75] Security screenings are thus possible, provided that they respect the provisions of the applicable treaties. Several other States have also over the past years added further restrictions to access their market, notably through the addition of security screening and review procedures for investments in the digital economy and more specifically for investment in communication networks and services.[76]

Finally, while the 2012 US Model BIT authorises the submission of claims to arbitration in relation to allegations of breaches of investment authorisations,[77] other treaties containing market access provisions precisely remove such question from the States' consent to arbitration. For example, Article II(4)(a) of the Canada-Egypt BIT carves out decisions relating to whether or not to permit an acquisition from the provisions of Articles XIII [Settlement of Disputes between an Investor and the Host Contracting Party] or XV [Disputes between the Contracting Parties].[78]

This precise provision was the subject of a very recent decision[79] relating to a national security screening and review decision by Canada. The national security screening was based on the 'Investment Canada Act' which provides for specific regulations and conditions for admission to the Canadian market.[80] This screening had prevented Global Telecom Holding from acquiring a Canadian telecom operator because of concerns about one of Global Telecom Holding's shareholders, which reportedly was owned by Russian investors and which made use of equipment by the Chinese manufacturer Huawei.[81] The tribunal, however, by majority, considered that under the specific facts of the case, the acquisition of control by Global Telecom Holding over Wind Mobile was not an 'acquisition' in the sense of Article II(4)(a) of the Canada-Egypt BIT.[82] The tribunal thus confirmed jurisdiction.

---

[74] Ibid., Art 14(2).

[75] Treaty between the Government of the United States of America and the Government of the State of Bahrain concerning the encouragement and reciprocal protection of investment (signed 29 September 1999, entered into force 30 May 2001) (Bahrain-US BIT) (2000) Art 2, Annex.

[76] See World Investment Report 2016 (n 67) 96.

[77] US Model BIT (n 73) Art 24(1)(a)(i)(C).

[78] Agreement Between the Government of Canada and the Government of the Arab Republic of Egypt for the promotion and protection of investments (signed 13 November 1996, entered into force 3 November 1997) (Canada-Egypt BIT) Art II.

[79] *Global Telecom Holding SAE v Canada*, ICSID Case No ARB/16/16, Award of the Tribunal (27 March 2020).

[80] For an overview, see World Investment Report 2016 (n 67) 96.

[81] Damien Charlotin, 'Analysis: in Global Telecom v Canada, arbitrators unanimously reject FET, FPS and free transfer claims, but disagree on national treatment argument and national security exception', *IAReporter* (29 April 2020) https://www.iareporter.com/articles/analysis-in-global-telecom-v-canada-arbitrators-unanimously-reject-fet-fps-and-free-transfer-claims-but-disagree-on-national-treatment-argument-and-national-security-exception/ accessed 15 May 2020.

[82] *Global Telecom Holding SAE* (n 79) para 328.

3. APPLYING INVESTMENT PROTECTION STANDARDS IN CYBERSPACE

Moving to the substantive part of international investment law, two distinct types of situations deserve special consideration. The first question is to what extent measures taken by the host State in the area of cybersecurity can, if harmful to the investment, result in a successful investment treaty claim by the harmed foreign investor. Secondly, in the event of cyberattacks on or cybersecurity issues related to the assets of foreign investors, the role and responsibility of the host State in which the foreign investor has invested may result in an investment claim brought by the targeted foreign investors. The question then is to what extent an international investment treaty may successfully be used to remedy the damage caused by cyberattacks. The question will be to what extent the State can be held responsible firstly for the cyberattack itself, and secondly, for not having exercised the necessary due diligence to prevent such a cyberattack and/or to bring the perpetrators to justice.

I will look at both questions from the perspective of two investment treaty provisions regularly found in international investment treaties: FET and FPS.[83] Both provisions will be predominantly, but not exclusively, relevant for one of the two particular situation: FET mostly will be relevant for the question of harm caused by the adoption of cybersecurity regulations, while FPS mostly will apply in case of cyberattacks on the assets of foreign investors.[84]

3.1 Fair and Equitable Treatment and Cyber Regulations

3.1.1 The FET standard

FET generally is referred to as a non-contingent, absolute standard of treatment as opposed to contingent, relative standards, such as NT. Absolute standards ask the State to act in a certain way as required under international law, irrespective of how other investors or investments are treated. The obligation to treat foreign investors fairly and equitably is stipulated in the vast majority of BITs.[85]

The FET standard clearly is a flexible and rather vague concept, but case law and scholarship have considered the following obligations to form part of FET: observance of the investor's legitimate expectations, non-discrimination, proportionality, due process, transparency, freedom from coercion and harassment, stability, predictability and a general duty of due diligence.[86]

---

[83] The exact relation between FPS and FET, and the so-called 'international minimum standard' (IMS) is still subject to much debate, but I do not intend to engage in that question. See for a discussion Christoph Schreuer, 'Full Protection and Security' (2010) 1 *Journal of International Dispute Settlement* 353.

[84] While some authors have also explored the question of direct or indirect expropriation of digital assets in the context of cyber-theft and economic espionage, the challenges and difficulties in invoking such a provision are important and hence I will not discuss it here. See Chaisse and Bauer (n 15) 585–7.

[85] Roland Kläger, 'Fair and Equitable Treatment: A Look at the Theoretical Underpinnings of Legitimacy and Fairness' (2010) 11 *The Journal of World Investment & Trade* 436.

[86] Andrew P Newcombe and Lluis Paradell, *Law and Practice of Investment Treaties: Standards of Treatment* (Kluwer Law International 2009) 277–9; Ioana Tudor, *The Fair and Equitable Treatment Standard in the International law of Foreign Investment* (OUP 2008) 157, 186; Kläger, ibid. See also for an overview of the contents of the standard in function of arbitral practice: Katia Yannaca-Small,

While there are different models and formulations of FET clauses,[87] I will here focus only on the question whether certain sub-components of the FET standard – without taking a position on whether or not these components are by necessary implication always part of the FET standard in all treaties – may provide a basis for a claim in relation to regulations in the cyber sphere. The requirement of a stable legal framework, the legitimate expectations of the foreign investor, and the prohibition of arbitrary and unreasonable measures seem to be most relevant here.

3.1.2 The FET standard and cyber regulations

While general regulations can be adopted by the host State affecting foreign investors, and hence can result in the initiation of an investment treaty claim, host State regulatory activity in relation to digital activities may present specific challenges. Besides general regular activities of States which may be found in breach of investment treaty obligations, government policies and regulations in a digital investment environment may require specific regulation to address issues such as privacy and data protection, consumer protection for e-commerce, content restrictions, the protection of intellectual property rights, or data location requirements obliging digital business to store local data within a specific country because of privacy and national security considerations.[88]

Regulations in those areas, of course, may not be legally problematic in and of themselves, and hence may be compatible with the State's obligations under international investment treaties. While the digital business environment may require specific regulatory activity, and while such regulations may be more prone to rapid changes,[89] the idea that States, in general terms, have the right to regulate, including in relation to digital businesses, remains unaffected as a matter of principle. In this respect, there is, in the practice of arbitral tribunals, a tendency to a more cautious approach to FET through the recognition of the States' right to regulate and thus for States to maintain sufficient regulatory space.[90] A certain regulation or measure adopted by the State relating to social or consumer protection may thus fall under the exercise by the State of its right to regulate in the public interest.

However, one cannot exclude that the imposition of certain requirements and regulations which impact foreign investments negatively may be considered a breach of certain investment protection standards, such as FET. It has for instance been argued that regulations adopted by a State in the pursuit of the regulation of cyberspace and providing cybersecurity, such as source code disclosure, or limitations to cross-border dataflows[91] may be captured

---

'Fair and Equitable Treatment Standard: Recent Developments' in August Reinisch (ed), *Standards of Investment Protection* (OUP 2008) 118 *ff*.

87 See Dolzer and Schreuer (n 11) 132 *ff* and Eric De Brabandere, 'States' Reassertion of Control over International Investment Law – (Re)Defining 'Fair and Equitable Treatment' and 'Indirect Expropriation' in Andreas Kulick (ed), *Reassertion of Control over the Investment Treaty Regime* (CUP 2016) 285–308.

88 See, also for a more complete list of areas of regulation: World Investment Report 2017 (n 16) 207–9.

89 Chaisse and Bauer (n 15) 572.

90 See for a discussion also Ursula Kriebaum, 'FET and Expropriation in the (Invisible) EU Model BIT' (2014) 15 *The Journal of World Investment & Trade* 471. See also Consolidated CETA Text (26 September 2014) art 8.9(1) http://trade.ec.europa.eu/doclib/docs/2014/september/tradoc_152806.pdf accessed 7 June 2020.

91 Chaisse and Bauer (n 15) 570.

by several components of FET. Also, there have been reports on possible claims by Chinese investor Huawei in relation to assertions by the Czech Republic that the telecom company's 'technologies and equipment pose a security threat'.[92]

Despite the specificity of regulating the digital economy, acts of the State in breach of the State's investment treaty obligations will be assessed by reference to the usual understandings and interpretations of investment treaty provisions. Since there have not yet been any investment dispute submitted to arbitration or any other type of settlement in relation to the harm caused by cybersecurity regulations, it is difficult to provide any firm answer as to whether such regulations might constitute a breach of FET. Indeed, applying FET to regulations is very fact-specific and will inevitably depend on the precise formulation of the regulations, the general objective and context of their adoption, their scope of application, and their impact on the investment. An important aspect also might be whether regulations or acts target one specific investor or apply more broadly to all investors investing in a certain territory.

Measures taken by the host State which are unreasonable and arbitrary, for instance because the decision is not based on 'legal standards, but on discretion, prejudice or personal preference', or that is taken 'for reasons that are different from those put forward by the decisions maker',[93] have been considered in breach of the FET standard. In relation to consistency and legitimate expectations, it is clear, also in the context of investment in digital assets, that 'the state is certainly not responsible for all the imaginable factors that could frustrate an investor's legitimate expectations'.[94] For instance, foreign investors cannot expect that the host State would not alter existing or adopt new cyber-related legislation, especially if it responds to certain genuine concerns. There is also no general stabilisation requirement, in the sense that the host State would not be able to make changes to the regulatory environment, or to be more precise be held liable under the investment treaty if it were to do so.[95] Yet, it remains that a State should generally respect the expectations resulting from the host State's conduct in respect of commitments or representations made by the State.[96]

3.2 (Full) Protection and Security, and Cyberattacks

3.2.1 The FPS standard

Provisions granting protection and security to investments and investors vary in nature. Some treaties refer to 'full protection and security', while others provide for 'protection and security' or 'constant protection and security'. It is not the purpose here to engage in a discussion of these variances. Thus, the standard will be referred to here as FPS despite the existing different

---

[92] Jarrod Hepburn and Luke Eric Peterson, 'Analysis: as Huawei invokes investment treaty protections in relation to 5G network security controversy, what scope is there for claims under Chinese treaties with Czech Republic, Canada, Australia and New Zealand?', *IAReporter* (11 February 2019) 1 www.iareporter.com/articles/analysis-as-huawei-invokes-investment-treaty-protections-in-relation-to-5g-network-security-controversy-what-scope-is-there-for-claims-under-chinese-treaties-with-czech-republic-canada-australia-a/ accessed 7 June 2020.

[93] Dolzer and Schreuer (n 11) 193.

[94] Salacuse (n 20) 255.

[95] Ibid., 255.

[96] Newcombe and Paradell (n 86) 279.

wordings. Some tribunals moreover have argued that the differences in wording do not make a substantive difference.[97]

In principle, the obligation to provide protection and security covers both an obligation for the State itself to abstain from infringing the physical protection and security of aliens, which applies to all State organs and entities the acts of which are attributable to the State, and an obligation of due diligence in relation to acts of third-parties other than State organs. The State's duty to abstain itself is not tested by reference to the due diligence standard.[98] In that case, contrary to the responsibility of States for acts of third parties other than State organs, the wrongful act is *the act that has caused harm*.

Conversely, in case of acts of third parties other than State organs, the internationally wrongful act is *the failure to prevent* the occurrence of the act or the failure to apprehend or punish those responsible for the act. The breach of that obligation, then, is assessed through the due diligence standard and implies no strict liability for the host State.[99] This applies equally to the obligation for States to act with due diligence to apprehend and punish those responsible for the act, which also is part of the FPS standard.[100] In the words of the tribunal in *El Paso v Argentina*, States have a duty of prevention and a duty of repression.[101]

Besides the requirement of providing physical protection and security, certain tribunals have, in particular when the word 'full' precedes 'protection and security', extended the application of the standard to 'legal protection and security', making this understanding of the standard in fact relatively similar to the FET standard.[102] Legal protection and security, in certain interpretations, in essence would require States to refrain from taking legal or governmental acts or measures that would hinder the proper functioning of the investment or would contravene investor's rights.[103] Certain case law suggests that FPS requires host States to provide to foreign investors a legal framework that guarantees legal protection to investors.[104] Others however, have limited the scope of the provision to the more traditional understanding of physical protection and security.[105]

---

[97] *Parkerings-Compagniet AS v Republic of Lithuania*, ICSID Case No ARB/05/8, Award (11 September 2007) para 354.

[98] Riccardo Pisillo-Mazzeschi, 'The Due Diligence Rule and the Nature of the International Responsibility of States' (1992) 35 *German Yearbook of International Law* 23.

[99] Salacuse (n 20) 132, 209–10. See also *Asian Agricultural Products Ltd v Republic of Sri Lanka*, ICSID Case No ARB/87/3, Final Award (27 June 1990) para 77.

[100] Campbell McLachlan, Laurence Shore and Matthew Weiniger, *International Investment Arbitration: Substantive* Principles (OUP 2008) 262, para 7.190 and Newcombe and Paradell (n 86) 246, para 6.8.

[101] *El Paso Energy International Company v The Argentine Republic,* ICSID Case No. ARB/03/15, Award (31 October 201) para 523.

[102] For a discussion, see Eric De Brabandere, 'Host States' Due Diligence Obligations in International Investment Law' (2015) 42 *Syracuse Journal of International Law and Commerce* 319.

[103] See, for a discussion, Schreuer (n 83).

[104] Ibid., 363.

[105] *Noble Ventures, Inc v Romania*, ICSID Case No ARB/01/11, Award (12 October 2005) para 164. Since the 'legal' aspect of FPS is very close to the FET standard, I will not discuss that aspect of FPS here. Indeed, the requirement that States should refrain from taking legal or governmental acts or measures that would hinder the proper functioning of the investment or would contravene investor's rights adds little to what has been discussed above in relation to FET.

3.2.2 FPS and cyberattacks

Before turning to the obligations of States in relation to cyberattacks, it is important to first analyse whether at all FPS obligations can apply to intangible assets, such as digital assets. I do not consider this question to be necessarily linked to the issue of whether FPS covers not only 'physical or police protection' but also *legal* protection which more broadly could apply to tangible and intangible assets. Rather, the question is whether the 'physical' aspect of FPS can be interpreted so as to cover 'police protection' in relation to intangible assets, and thus whether this aspect of FPS can be effectively used to cover host State measures, or lack thereof, in case of cyberattacks on the foreign investor's digital assets.

While it has been considered that it is 'difficult to understand how the physical security of an intangible asset would be achieved',[106] the argument has been made that to make the FPS effective in case of intangible assets of foreign investors, the 'traditional assurances offered by the common FPS standard must be enlarged'.[107] In this context, applying FPS to digital assets does not necessarily need to imply that FPS is intended to cover 'legal' protection and security in general. Indeed, if one goes back to the original purpose and origins of the FPS standard,[108] it becomes clear that it was mainly intended to protect the physical integrity of investments against interference by the 'use of force'.[109] The 'use of force' was historically targeting acts of a criminal nature, such as isolated acts of individuals relating to the theft of parts of locomotives,[110] acts of the State in relation to the killing of a family member by a third party,[111] or acts in relation to mob violence, riots or civil unrest,[112] and insurrectional movements.[113]

Based on this, one could argue that the essence of FPS is not only to protect the tangible assets of foreign investors, but rather a more general duty for the State to prevent harmful acts of third parties from violence by third parties and its own organs. In such case, the transposition of the more traditional conception of FPS as covering 'physical protection' of foreign investors' tangible assets to include also protection in case of cyberattacks on digital assets is easier to argue and does not need to engage in the question on the expansion of PFS to 'legal' protection and security.[114]

---

[106] *Siemens AG v The Argentine Republic*, ICSID Case No ARB/02/8, Award (17 January 2007) para 303.

[107] Collins (n 5) 236.

[108] See De Brabandere (n 102).

[109] *Saluka Investments BV v The Czech Republic*, UNCITRAL, Partial Award (17 March 2006) para 484.

[110] General Claims Commission (Mexico and United States), *H G Venable (USA) v United Mexican States*, Decision of 8 July 1927, IV UNRIAA 219-261.

[111] General Claims Commission (Mexico and United States), *Laura M B Janes et al (USA) v United Mexican States*, Decision of 16 November 1925, IV UNRIAA 82-98.

[112] *Affaire des biens britanniques au Maroc espagnol (Espagne contre Royaume-Uni) (British Property in Spanish Morocco)*, Decision of 1 May 1925, II UNRIAA 615, 642, 645. See also Great-Britain United States Mixed Commission, *Home Frontier and Foreign Missionary Society of the United Brethren in Christ,* Decision of 18 December 1920, IX UNRIAA 144.

[113] Mixed Claims Commission (Italy-Venezuela)*, Sambiaggio Case* (1903) X UNRIAA 499, 524.

[114] Moreover, if one looks at contemporary treaties which refer to the FPS standard in its relation to customary law, one can see that the FPS standard is directly linked to 'police protection', without references to mob violence, riots or civil unrest, and insurrectional movements, or to tangible assets only. See e.g., US Model BIT (n 73) Art 5(2)(b).

If we extrapolate and try to apply these general principles to the specific context of cyberattacks and cybercrime, it is necessary to keep in mind that digital assets often exist in conjunction with some form of physical infrastructure. The application of FPS to the latter is more straightforward, in the sense that the obligation for the host State to physically protect the tangible assets of the foreign investor is very much in line with the contemporary conception of FPS and existing case law on the subject.[115] I will thus focus here generally on the obligations towards digital assets generally.

To turn to the application of the FPS standard: the State itself of course is first responsible for not engaging in cyberattacks against foreign investors who have invested on the State's territory, and will be responsible under the investment treaty if such would occur. But more importantly, in the context of cyberattacks, the responsibility of the State under the FPS standard involves exercising due diligence to prevent cyberattacks by third parties and to apprehend and punish those responsible for the acts.[116]

In general, establishing precise obligations of States to act in due diligence to prevent cyberattacks on foreign investors' digital assets is challenging. First of all, and contrary to tangible assets located in the territory of the host States, the precise location of the digital assets is difficult to determine. One criterion can be the location of the server that hosts the digital assets for the foreign investor, which probably is the most straightforward one, since it also links the obligation to the notion of investment 'in the territory' of the host State.[117] Applying that criterion, it has been argued that States would have an obligation to 'ensure that the websites which it hosts are not attacked'.[118] But the difficulty is that foreign investors' digital assets are, as most digital assets, managed through internet service providers which are private entities,[119] and it seems difficult to argue that States would have a general obligation – even of due diligence – to prevent cyberattacks targeting specific investors' digital assets or websites which are stored on or located on servers held or managed by non-State internet service providers. For instance, contrary to the State's possibility to send police forces to an investor's facilities which are on the verge of an attack by a mob, it is more difficult to imagine how a State could exercise due diligence to prevent a cyberattack on that same investor's digital systems located on servers hosted by private parties.[120]

However, the argument has been made that the State would be under a general obligation to provide a certain form of internet security, and notably for those parts of the cyberspace where the State can in fact intervene. One can think of the internet infrastructure generally, or the stability of communications networks.[121] Here again, however, much depends on whether or

---

[115] See e.g., *Ampal-American Israel Corporation and others v Arab Republic of Egypt*, ICSID Case No ARB/12/11, Decision on Liability and Heads of Loss (21 February 2017) paras 235 *ff*.

[116] Even beyond the FPS standards, it has been argued that States may have an obligation of prevention and cessation in relation to cyberattacks committed by enterprises on their territory. See Philippe Achilleas, 'Entreprises, cyberattaques et responsabilité. Aspects de droit international et européen' in Frédérick Douzet, *Cyberattaques et droit international – Problèmes choisis* (Pedone 2018) 148 and Claire Crépet-Daigrement, 'Responsabilité de l'Etat-auteur d'une cyberattaque' in Douzet, ibid., 161.

[117] Collins (n 5) 237.

[118] Ibid.

[119] Ibid.

[120] Cf. ibid., 238.

[121] Ibid.

not the general infrastructure is in the hands of the State or agencies of the State and whether any action by the State is possible at all.

The State's obligation to exercise due diligence to apprehend and punish those responsible for cybercrime or cyberattacks may play an important role also. This requires from the State to make available to the foreign investors, its legal, judicial and administrative apparatus to detect and effectively prosecute those responsible. The obligations imply also an obligation of due diligence to investigate cyberattacks and, where possible, use all prosecutorial means available to bring the perpetrator to justice.[122] Here also, the fact that we are dealing with cybercrime implies that the effectiveness of such an obligation may prove difficult to implement in practice: the origins of cyberattacks, and the capacity to bring to justice foreign perpetrators is not straightforward and may fail on jurisdictional grounds. And one should keep in mind that the obligation is one of due diligence, not of strict liability. Can one expect from a State to create special mechanisms only for the protection of foreign investors' digital assets? The due diligence standard, in turn, implies that liability might be easier to find in case of evident and predictable attacks.[123]

4. CYBERSECURITY AND SECURITY EXCEPTIONS IN INTERNATIONAL INVESTMENT LAW

After having discussed the possible claims foreign investors may have in relation to investments in cyberspace, one needs to consider whether, in the event of a breach of the applicable investment treaty, such a breach may fall under a so-called 'security exception' often contained in investment treaties. Much has already been written on security clauses in international investment treaties, notably because of their use as a defence against responsibility in relation to the Argentinian economic and financial crisis in the late 1990s and early 2000s, and the subsequent divergent decisions of arbitral tribunals in that respect.[124]

In general, measures taken by the host State in the post-entry stage which are in breach of the investment protection provisions in that treaty – mostly under the FET standard of treatment in case of adoption of cybersecurity legislation – might be covered by the security exception of the treaty and hence result in a finding of conformity with the treaty nonetheless.[125]

There are a variety of exceptions which potentially can come into play. I will first look at security exception clauses in BITs, also called 'non-precluded measures provisions', before turning to circumstances precluding wrongfulness under the general customary norms relating to State responsibility.

---

[122] See De Brabandere (n 102) 319, 340.

[123] Levon Golendukhin, 'Chapter 6 - Full Protection and "Cyber" Security? (Panel Discussion)' in Ian A Laird and others (eds), *Investment Treaty arbitration and International Law* (Juris 2018) 137.

[124] See amongst others: Giorgio Sacerdoti, 'The Application of BITs in Time of Economic Crisis: Limits to their Coverage, Necessity and the Relevance of WTO Law' in Giorgio Sacerdoti (ed), *General Interests of Host States in International Investment Law* (CUP 2014) 3–25. More generally, see Caroline Henckels, 'Investment Treaty Security Exceptions, Necessity and Self-defence in the Context of Armed Conflict' in Katia Fach Gómez, Anastasios Gourgourinis and Catharine Titi (eds), *European Yearbook of International Economic Law: International Investment Law and the Law of Armed Conflict* (Springer 2019) 319–40.

[125] Wang (n 69) 70.

4.1 General Security Exception Clauses

Many investment treaties, but clearly not all,[126] include a provision aimed at excluding certain measures from potentially constituting a breach of the investment treaty. An example of such a clause is Article 12(2) of the India-Serbia BIT:

> […] nothing in this Agreement precludes the host Contracting Party from taking action for the protection of its essential security interests or in circumstances of extreme emergency in accordance with its laws normally and reasonably applied on a non discriminatory basis.[127]

Other treaties are slightly more detailed, such as the 2012 US Model BIT,[128] or specify the areas for which legislation and regulation is carved out.[129]

It has been noted that, while such clauses conform to an understandable need to carve out legislative and regulatory measures necessary to safeguard important national interests, the usual vagueness and generality of the terms leaves the door open for an unjustified reliance on them.[130] This may be even more the case if the clause is intended to be of a self-judging nature,[131] such as Article 18(2) of the US Model BIT which provides that the treaty shall not be construed as to preclude a party from applying measures 'that it considers necessary'.[132]

Without wanting to engage in a full analysis of the question of the application and precise scope of essential security interest clauses, it is of course important to point out that in case the State is successful in arguing that the measures were necessary to protect the State's essential security interests, the measures would indeed not be in violation of the treaty since the treaty's substantive protection obligations of the State do not apply.[133] The application of the clause to FPS would be more difficult, since the State would have to argue quite paradoxically that the lack of due diligence in preventing an attack or in finding and prosecuting those responsible for the attack would be necessary to maintain its essential security interests.

While such clauses have not yet been tested in the specific context of cybersecurity legislation, there have been several reports of possible claims by Chinese investor Huawei in relation to assertions by the Czech Republic that the telecom company's 'technologies and equipment

---

[126] See e.g., Treaty between the Federal Republic of Germany and the Republic of Venezuela for the promotion and reciprocal protection of investments (signed 14 May 1996, entered into force 16 October 1998) (Germany-Venezuela BIT).

[127] Agreement between the Government of the Republic of India and the Federal Government of the Federal Republic of Yugoslavia for the reciprocal promotion and protection of investments (signed 31 January 2003, entered into force 24 February 2009) (India-Serbia BIT) Art 12(2).

[128] US Model BIT (n 73) Art 18(2).

[129] Agreement for the promotion and protection of investments between the Republic of Colombia and the Republic of India (signed 10 November 2009) (Colombia-India BIT) Art 13.

[130] Salacuse (n 20) 379.

[131] The precise effects of a self-judging clause on the competence of an arbitral tribunal to review the reliance by the State on the clause is still open to much debate. For a discussion see Stephan Schill and Robyn Briese '"If the State Considers": Self-Judging Clauses in International Dispute Settlement' (2009) 13 *Max Planck Yearbook of United Nations Law* 61.

[132] US Model BIT (n 73) Art 18(2).

[133] *CMS Gas Transmission Company v Argentine Republic*, ICSID Case No ARB/01/8, Decision of the Ad Hoc Committee on the Application for Annulment of the Argentine Republic (25 September 2007) para 129.

pose a security threat'.[134] While no claims have been filed at this stage, it is interesting to note that the China-Czech Republic BIT contains no security clause. Other States such as Canada, Australia and New Zealand have 'closed the doors on Huawei involvement in building national 5G networks'[135] and most of the investment treaties signed between China and these States also do not contain an essential security clause. However, as was discussed earlier in relation to another BIT involving Canada, in the case of the Canada-China BIT the treaty does carve out security screening from investor-State arbitration in relation to a decision by Canada following a review under the Investment Canada Act, whether or not to 'initially approve an investment that is subject to review', or to 'permit an investment that is subject to national security review'.[136]

But the general question whether security exceptions could apply to regulations which would cause harm to certain investors because they are considered 'security risks' is worth exploring. Two recent and related cases deserve attention, since they map out quite clearly the possibilities of the use of essential security interests clauses in relation to cybersecurity. The cases involved investments in the telecom sector in India, and were not related to cybersecurity, but the question whether the essential security interests clause could be relied on by India was discussed in detail in both cases. In both cases,[137] a Mauritian (CC Devas) and a German investor (Deutsche Telekom) had participated in an 'Agreement for the Lease of Space Segment Capacity' with an Indian State-owned enterprise in order to offer 'broadband wireless access and audio-video services throughout India'.[138] The dispute related to the cancellation of that agreement following a 'policy decision taken by the Government of India to reserve a part of the electromagnetic spectrum known as the S-band "for national needs, including for the needs of defence, para-military forces, railways and other public utility services as well as for societal needs, and having regard to the needs of the country's strategic requirements"'.[139]

In both cases India relied on the differently worded 'essential security interests' clauses in the respective applicable treaties.[140] In *CC Devas*, the tribunal, by majority, considered after a lengthy analysis that the decision to reserve a part of the electromagnetic spectrum only was partly 'directed to the protection of its essential security interests', the other part being subjected to the investment protection standards in the treaty.[141] The tribunal, in its decision, however accepted that it should give the State a 'wide measure of deference':

> An arbitral tribunal may not sit in judgment on national security matters as on any other factual dispute arising between an investor and a State. National security issues relate to the existential core

---

[134] Hepburn and Peterson (n 92) 1.

[135] Ibid., 2.

[136] Agreement Between the Government of Canada and the Government of the People's Republic of China for the promotion and reciprocal protection of investments (signed 9 September 2012, entered into force 1 October 2014) (Canada-China BIT) Annex D.34.

[137] *CC/Devas (Mauritius) Ltd, Devas Employees Mauritius Private Limited and Telecom Devas Mauritius Limited v India*, PCA Case No 2013-09, Award on Jurisdiction and Merits (25 July 2016) and *Deutsche Telekom v India*, PCA Case No 2014-10, Interim Award (13 December 2017).

[138] For the facts of the cases, see, *CC/Devas (Mauritius) Ltd*, ibid., paras 5 *ff*.

[139] Ibid., para 6.

[140] In *CC Devas v India,* Art 11(3) of the Agreement between the Government of the Republic of Mauritius and the Government of the Republic of India (signed 4 September 1998, entered into force 20 June 2000, terminated on 22 March 2017) (Mauritius-India BIT) applied.

[141] *CC/Devas (Mauritius) Ltd* (n 137) para 371.

> of a State. An investor who wishes to challenge a State decision in that respect faces a heavy burden of proof, such as bad faith, absence of authority or application to measures that do not relate to essential security interests.[142]

In *Deutsche Telekom v India*, the applicable BIT's clause was formulated slightly differently and included the term 'to the extent necessary' before 'for the protection of its essential security interests'.[143] The tribunal noted that the question whether a measure is 'necessary for the protection' of a State's essential security interests, is 'subject to review by the Tribunal'.[144] In reviewing the decisions, the tribunal considered that it will:

> undoubtedly recognize a margin of deference to the host state's determination of necessity, given the state's proximity to the situation, expertise and competence. Thus, the Tribunal would not review de novo the state's determination nor adopt a standard of necessity requiring the state to prove that the measure was the 'only way' to achieve the stated purpose. On the other hand, the deference owed to the state cannot be unlimited, as otherwise unreasonable invocations of Article 12 would render the substantive protections contained in the Treaty wholly nugatory. [145]

The tribunal also explained that it will examine whether 'the measure was principally targeted to protect the essential security interests at stake and was objectively required in order to achieve that protection, taking into account whether the state had reasonable alternatives, less in conflict or more compliant with its international obligations'.[146] In the end, the tribunal, contrary to the decision in *CC Devas*, argued that India failed to establish that the decision was 'necessary to protect those essential security interests'.[147]

These two recent cases show that the invocation by a State of essential security interests as a shield against treaty claims is not straightforward. Notably, much discussion still exists as to the appropriate standard applicable to the review by the tribunal, which of course depends also on the specific formulation of the clause.

4.2 Circumstances Precluding Wrongfulness

Since not all treaties include a provision aimed at excluding certain measures from potentially constituting a breach of the investment treaty because of 'essential security interests', the customary law circumstances precluding wrongfulness as embodied in the ILC Articles on States Responsibility may play an important role.

The dozens of cases initiated against Argentina in the 2000s following the State's economic and financial crisis, in which Argentina has systematically invoked both the treaty-specific essential security interests clauses and the customary norm of 'necessity' as a circumstance precluding wrongfulness, have resulted in a series of decisions relating to the precise relation

---

[142] Ibid. para 245.

[143] Agreement between the Federal Republic of Germany and the Republic of India for the promotion and protection of investments (signed 13 July 1998, entered into force 13 July 1998, terminated on 3 June 2017) (Germany-India BIT) art 12.

[144] *Deutsche Telekom* (n 137) para 238.

[145] Ibid.

[146] Ibid., para 239.

[147] Ibid., para 285.

between both. The decision of the Annulment Committee in *CMS v Argentina*[148] was one of the first to attempt to clarify the precise relation between both norms, thereby departing from decisions which had argued that the treaty-specific essential security interests clauses should be interpreted in light of the customary norm on necessity.[149] The Committee established that both provisions are formulated differently and contain different requirements.[150] It then confirmed that the 'state of necessity in customary international law goes to the issue of responsibility', which makes it a secondary rule of international law.[151] In other words, tribunals confronted with the invocation of both provisions – the treaty norm and the customary norm of necessity – would be under an obligation to consider first whether the breach of the BIT was excluded by the essential security interests clause, and if that was not the case, whether responsibility could be precluded in whole or in part under customary international law.[152]

Irrespective of the position taken on the precise relation between the two, it is clear that both provisions are formulated differently. It has been made clear on various occasions that the requirements under Article 25 of the ILC Articles are stricter than those under the usual essential security interests clauses found in BITs.[153] The invocation of necessity, as codified in Article 25 of the ILC Articles on State Responsibility, requires amongst others, that a certain act 'is the only way for the State to safeguard an essential interest against a grave and imminent peril' and it may not be invoked if 'the State has contributed to the situation of necessity'. Essential security interests clauses, however, usually are formulated in such a way as to exclude the application of the protection standards to protect an 'essential security interest'.

As the Argentinian cases have shown, tribunals have confirmed that as a matter of principle, an economic crisis may give rise to a plea of necessity under customary international law, and there is no reason to doubt that such may not be the case in the event of acts or measures taken in the event of a cybersecurity crisis. However, pleas of necessity are in general very hard to make and therefore succeed only very occasionally.[154] This will be no different in case of claims by States that the wrongfulness of certain acts adopted in the cybersecurity context, found in breach of investment protection standards, is precluded because it was 'the only way for the State to safeguard an essential interest against a grave and imminent peril'. Moreover, the requirement that the plea of necessity may not be invoked if 'the State has contributed to the situation of necessity' could also be pivotal. Certain tribunals in the context of the Argentinian crisis indeed have argued that necessity may not be invoked because 'government policies and their shortcomings significantly contributed to the crisis and the emergency'.[155]

---

[148] *CMS Gas Transmission Company* (n 133).

[149] See for a discussion see Dolzer and Schreuer (n 11) 189.

[150] *CMS Gas Transmission Company* (n 133) para 130.

[151] Ibid., para 134.

[152] Ibid., para 134. For a criticism of the decision on these issues, and for other cases which have departed from the *CMS Committee's decision,* see Dolzer and Schreuer (n 11) 189.

[153] *Deutsche Telekom* (n 137) para 229.

[154] David Collins, *An Introduction to International Investment Law* (CUP 2020) 303.

[155] *CMS Gas Transmission Company v Argentine Republic*, ICSID Case No ARB/01/8, Award (12 May 2005) para 329.

CONCLUSION

This chapter has attempted to give an overview of the main issues related to foreign investment in cyberspace. The 'cyber' nature of the assets involved, as has been shown, presents several distinct challenges to the use of investment protection standards in international investment treaties.

First, digital assets need to qualify as 'investment' under the applicable investment treaty, and in case of ICSID Arbitration, also under the notion of 'investment' contained in Article 25 ICSID Convention. The digital and hence intangible nature of investments in cyberspace presents peculiarities, but as I have shown, the broadness of definitions in investment treaties does not seem to exclude digital assets *per se*. However the usual limitations to acknowledging certain investments as such, remain applicable, both for definitions in investment treaties and under the ICSID Convention. Secondly, the admission and establishment of foreign investors in the digital economy might be subjected to restrictions. Even if treaties accept a limited right of admission by extending NT and MFN treatment to the admission of the investment, sectors such as a telecommunication are often excluded.

Based on the hypothesis that digital assets are 'protected investments' under the applicable international investment treaties, either individually or taken as a whole with other components of an investment operation, the question I have addressed is what protection international investment treaties may offer in case of harm caused to the investment in the event of cyberattacks on the assets of foreign investors, or in case of cybersecurity regulations and/or legislation adopted by the host State and which are harmful to the investment.

In light of increased cybersecurity concerns, States have increasingly adopted specific laws and regulations in relation to cybersecurity. Such legislation and regulations may, in certain situations, cause harm to investors and hence result in an invocation by the foreign investor of the State's obligations under investment treaties. I have noted that in such cases, the general principles applicable to most forms of investment apply, notably those under the FET standard of treatment. The requirements of stability, consistency, and transparency of the legal framework, the prohibition of arbitrary and unreasonable measures and the legitimate expectations of foreign investors if considered part of FET may play an important role.

In relation to cyberattacks, which I have discussed from the perspective of the FPS clause, a clear distinction needs to be made between attacks originating from the host State of the investment and attacks originating from a third country. The question will, in the first scenario, be to what extent the State can be held responsible for the cyberattack itself, and in the latter scenario for not having exercised the necessary due diligence to prevent such an cyberattack and/or bring the perpetrators to justice.

This chapter has also considered the possible invocation of 'essential security interests' clauses. Measures taken by the host State in the post-entry stage which are in breach of the investment protection provisions in that treaty – mostly under the FET standard of treatment in case of adoption of cybersecurity legislation – might be covered by the security exception of the treaty and hence result in a finding of conformity with the treaty nonetheless. This, I have noted, is still subject to much discussion, notably on the applicable standard of review of the tribunal. Moreover, circumstances precluding wrongfulness under the general customary norms relating to State responsibility may also play a role if the 'essential security interests' clause has been discarded by the tribunal.

10. Cyber terrorism and use of the internet for terrorist purposes

Ben Saul and Kathleen Heath

1. INTRODUCTION

To date there are few, if any, real-world examples of terrorist acts committed by 'cyber' means,[1] that is, through the use of computer networks. Much of the discussion of cyber threats has instead focused on other phenomena: sophisticated State cyber-attacks (such as Stuxnet against Iran); disruptive, but rarely dangerous, political 'hacktivism'; the use of the internet to commit cyber-crime or facilitate (but not to commit) terrorism; and the extent to which cyber acts constitute an 'armed attack' giving rise to self-defence, or are military 'attacks' on 'objects' regulated by international humanitarian law.

There are certainly conceivable risks of individuals or groups interfering electronically with computers, data, objects, infrastructure, or services in ways which terroristically harm people or property – for instance, to intimidate a population or coerce a government (which is the essence of a current draft UN treaty definition of terrorist offences).[2] Examples could include manipulating computer systems to: release flood water from a dam; disable water supplies or sewerage systems to endanger public health; disrupt transport signals to cause a train, aircraft, or vehicle to crash; or cease essential energy or gas supplies to hospitals or homes.

The threat of cyber-terrorism arises from the dependence of many States and their peoples on electronic systems, the internet and associated social, economic and physical infrastructure. The internet is a powerful, cheap, global, and potentially anonymous platform that is difficult to control but easy to exploit. As more critical infrastructure systems and essential services are moved online, security vulnerabilities increase.[3] The transnational architecture of the internet, and the anonymity it can provide, also pose difficult jurisdictional and evidentiary problems for law enforcement when seeking to trace perpetrators, attribute responsibility for attacks, and secure and preserve admissible evidence through mutual assistance. The lack of an agreed definition of cyber-terrorism, stemming in part from the absence of an agreed definition of terrorism, further impedes suppression and cooperation.

---

[1] Heather Harrison Dinniss, 'The Threat of Cyber Terrorism and What International Law Should (Try to) Do about It' (2018) 19 *Georgetown Journal of International Law* 43, 43.

[2] UN Draft Comprehensive Terrorism Convention, UNGAOR (68th Session), Supplement No 3: Report of the Ad Hoc Committee established by General Assembly Resolution 51/210, 17 December 1996, 16th session (8–12 April 2013) A/68/37, 6.

[3] See generally Counter-terrorism Implementation Task Force (CTITF), 'Countering the Use of the Internet for Terrorist Purposes' (CTITF Working Group Report, February 2009) 6; Hamadoun Touré, 'Cyberspace and the Threat of Cyberwar' in Hamadoun Touré, *The Quest for Cyber Peace* (International Telecommunications Union, January 2011) 7, 9–13; Darren Pauli, 'Hackers Gain 'Full Control' of Critical SCADA Systems', *IT News* (Australia, 10 January 2014) www.itnews.com.au/News/369200 ,hackers-gain-full-control-of-critical-scada-systems.aspx.

There is currently no international treaty to suppress 'cyber-terrorism', nor any agreed definition of it. There are also very few specific cyber-terrorism offences in national laws. Instead, there exists a patchwork of norms that only partially cover cyber-terrorism. Some acts of cyber-terrorism may be offences under the counter-terrorism conventions addressing certain means, methods or targets of terrorism, such as endangering the safety of civilian aircraft or shipping, among others. Further, the use of the internet to *facilitate* (but not perpetrate) terrorism may be captured by preparatory offences such as inciting, financing, recruiting for, or supporting terrorist acts (and States are required to implement such offences by Security Council resolutions). Regular cyber-crime offences under national law may also cover some cyber-terrorism, as well as certain uses of the internet to facilitate terrorism.

This chapter focuses on criminal law responses to cyber-terrorism, including through the existing sectoral treaties, the proposed Draft UN Comprehensive Terrorism Convention, and in regional and selected domestic criminal laws. It considers the adequacy of existing international law, including by comparison with the regional and domestic initiatives and in the light of policy discussions in UN forums. It concludes by asking whether it is necessary or desirable for the international community to take more direct legislative action against cyber-terrorism, or whether it is sufficient to rely upon the patchwork of general norms on terrorism and cyber-crime.

2. DEFINITION OF CYBER-TERRORISM

An immediate difficulty in confronting cyber-terrorism is the lack of an agreed legal definition of it. This has resulted in divergent and over-inclusive usages of the term, and uncertainty about its transnational legal regulation. Put simply, the adjective 'cyber' indicates that computer-based or electronic or digital means are employed to perpetrate a terrorist act, whether by harming computer systems themselves or using them as a conduit to attack dependent physical infrastructure in the 'real' world.

The United Nations Office of Drugs and Crime (UNODC) thus defines cyber-terrorism as the 'deliberate exploitation of computer networks as a means to launch an attack… intended to disrupt the proper functioning of targets, such as computer systems, servers or underlying infrastructure'.[4] The UN's Counter-Terrorism Implementation Taskforce (CTITF) similarly describes cyber-terrorism as the act of committing 'terrorist attacks by remotely altering information on computer systems or disrupting the flow of data between computer systems'.[5]

These definitions potentially encompass a variety of quite different situations. The situation most assimilable to conventional terrorism is where cyber methods cause harm to persons or property in the 'real' world, such as by interfering with the operating systems of air navigation, transport, public utilities (such as energy, water or sewerage) or essential services (such as hospitals). An example is the 'Stuxnet' computer worm attack on Iran's uranium enrichment program in 2010, which destroyed numerous centrifuges. A second situation is where the act causes physical harm to a computer/network (such as by disabling it) but without inflicting

4 UNODC, *The Use of the Internet for Terrorist Purposes* (2012) 11.
5 CTITF (n 3).

wider kinetic damage. An example is the computer virus attack on the Saudi Arabian State oil company Aramco in 2012, which disabled 3,000 computers.[6]

The third situation is where harm is caused purely to intangible data, such as operating software or code, or the integrity or confidentiality of information (such as economic, government, or personal information).[7] While attacks on the latter category do not strictly cause kinetic or physical harm in the real world, such attacks can potentially have more destructive effects than real world attacks – for example, if bank records, financial information, or stock holdings are manipulated or erased, causing major economic losses (and thereby potentially inducing, even in strong States, panic and social instability).

The adjective 'cyber' should not obscure the requirement that an act also fall within the legal definition of terrorism itself. Cyber-terrorism is not a new form of terrorism, but merely a 'new terrorist tactic'.[8] This begs the complex question of how 'terrorism' is defined or regulated in international law, including the well-known disagreements over 'State terrorism' and terrorism by national liberation movements. Not every interference with a computer system is cyber-terrorism; some interferences may be mere cyber-crime but not terrorism, while others may be legitimate dissent protected by international human rights law.

The discussion below accordingly focuses on 'terrorist' methods addressed by the counter-terrorism conventions (which focus on prohibited physical acts or their harmful consequences), before turning to the UN's proposed transnational crime of terrorism (which requires ulterior purpose elements of intimidation or coercion). It is first necessary, however, to distinguish cyber-terrorism proper from *the use of the internet to facilitate terrorism*, although both may be suppressed by resort to certain terrorism offences); as well to differentiate ordinary cyber-crime (which may be committed by terrorists).

A. (Mis)use of the Internet for Terrorist Purposes

Terrorist organisations may use the internet to recruit and train new members, organise and coordinate their activities, finance their operations, or incite terrorism or spread fear.[9] For example, to coordinate and execute the shooting and bombing attacks in Mumbai, India in 2008, terrorists used Global Positioning System (GPS) technology, mobile phones, satellite imagery and voice-over-internet-protocol phone numbers.[10] The Japanese cult Aum Shrinrikyo ('Supreme Truth') obtained sensitive online information about nuclear facilities in a number of countries in 2003.[11]

Further, since 2014 Islamic State has used the internet to publicly propagandize, radicalize, indoctrinate, recruit, incite, share information, raise funds, and threaten, but also for private, encrypted communications (including through social media apps) to coordinate their opera-

---

[6] Daniel Cohen, 'Cyber Terrorism: Case Studies' in Babak Akhgar, Andrew Staniforth and Francesca Bosco (eds), *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Elsevier 2014) 169.

[7] See e.g., Eric Luijf, 'Definitions of Cyber Terrorism' in Akhgar et al, ibid. 11, 14.

[8] Peter Fleming and Michael Stohl, 'Myths and Realities of Cyberterrorism' in Alex Schmid (ed), *Countering Terrorism Through International Cooperation* (2001) 30.

[9] These activities formed the focus of the UNODC's study (n 4). See also Bruno Halopeau, 'Terrorist Use of the Internet' in Akhgar et al (n 6) 123.

[10] Emily Wax, 'Mumbai Attackers Made Sophisticated Use of Technology', *Washington Post* (3 December 2008).

[11] Cohen (n 6) 166.

tions and preparations. The 'dark web' can also provide anonymous connectivity. In 2019, the far-right Christchurch mosque attacker 'live-streamed' footage on Facebook.

Both the Security Council and General Assembly have explicitly called on States to address the exploitation of the internet for terrorist purposes.[12] The Security Council has highlighted the use of the internet to incite, recruit, fund or plan terrorist acts,[13] and has emphasized the central role the internet has played in radicalizing individuals to terrorism, and in financing and facilitating the travel and subsequent activities of foreign terrorist fighters.[14]

Such predicate, precursor or preparatory activities are typically described as 'facilitative' of terrorism,[15] rather than constituting terrorist acts of themselves. However, a bright line cannot always be easily drawn between facilitation and commission. For example, a video post of a hostage may be a relevant fact in proving an element of the crime of hostage taking – namely, that the person's detention is to compel another to do something as condition of release.[16] Likewise, in the Christchurch attack, live-streaming could be evidence of the ulterior intention constituting a terrorist offence (under New Zealand law), namely to 'induce terror in a civilian population' or 'unduly compel or to force' a government to do or not do something.[17]

States are required to criminalize a range of relevant acts preparatory to or facilitative of terrorism, regardless of the means used; cyber-facilitation can thus fall within the scope of such measures. For example, Security Council resolution 1373 (2001) requires States to establish offences over 'any person who participates in the financing planning, preparation or perpetration of terrorist acts or in supporting terrorist acts'.[18] In national practice, 'support' and 'preparation' offences have been understood to encompass further offences relating to providing training, services, weapons, facilities or property; arranging meetings; recruiting; harbouring; soliciting; and participation (of many kinds) in terrorist organizations.

Moreover, resolution 1373 (2001) and the Terrorist Financing Convention 1999 criminalize the financing of terrorist acts by any means, specifically including where funds are raised and disbursed electronically.[19] Further, resolution 2178 (2014), criminalizes the financing, organizing, facilitating or recruiting for the travel of 'foreign terrorist fighters'.[20]

The Security Council has additionally recommended, but not required, that States criminalize other preparatory conduct, including: planning, training, financing or logistically supporting acts intended to destroy or disable critical infrastructure;[21] human trafficking to

---

[12] UN Security Council resolution 1373 (28 September 2001), [3(a)] (exchange operational information); UN Global Counter-Terrorism Strategy, UN General Assembly resolution 60/288 (20 September 2006), [II(12)(a)] (coordinate to counter it). In support of the latter resolution, the CTITF established a Working Group on Countering the Use of the Internet for Terrorist Purposes.

[13] UN Security Council resolution 2129 (17 December 2013, [14]).

[14] Security Council resolution 2178 (24 September 2014), preamble.

[15] Fleming and Stohl (n 8) 38.

[16] Hostages Convention 1979, art 1(1).

[17] Terrorism Suppression Act 2002 (New Zealand), s 5. It is an offence to commit a terrorist act under s 6.

[18] UN Security Council resolution 1373 (28 September 2001), [2(e)].

[19] The Terrorist Financing Convention 1999 makes it an offence to provide or collect funds with the intention or knowledge that they be used to carry out a terrorist offence.

[20] UN Security Council resolution 2178 (24 September 2014), [6].

[21] UN Security Council resolution 2341 (13 February 2017) [3].

support terrorism;[22] and trafficking in cultural property to benefit terrorist groups.[23] Finally, the Council has required States to prohibit (which could be implemented through offences, but this is not strictly required), certain other conduct, such as the acquisition of nuclear, chemical or biological weapons by non-State actors for terrorist purposes.[24] Again, the facilitation of any of the above conduct through the internet is implicitly captured by these stipulations.

Pertinently, Security Council resolution 1624 (2005) calls upon (but does not require) States to prohibit (but not strictly to criminalize) incitement to commit a terrorist act,[25] although any such offences adopted under national law must comply with human rights obligations to respect freedom of expression and religion.

One prominent example is found in European Union Directive 2017/541, which requires EU Member States to criminalize the distribution of public messages, online or offline, that are intended to incite terrorist offences, where such conduct advocates the commission of such offences.[26] Such advocacy may include where involves the 'glorification' of terrorist acts. Member States are also required to ensure the removal of online content that constitutes 'public provocation' to commit a terrorist offence that is hosted in their territory, or to block user access to this material in their territory.[27] The Directive further notes that self-study related to terrorism, including through the internet, 'should also be considered to be receiving training for terrorism when resulting from active conduct and done with the intent to commit or contribute to the commission of a terrorist offence'.[28]

More recently, following the prolific use of the internet by Islamic State in Iraq and Syria, attention has turned to the role of the private sector in countering the misuse of the internet. Security Council resolution 2396 (2017) stresses the need for cooperation between Member States, the private sector and civil society to prevent terrorists from exploiting technology and communications for terrorist acts.[29] The Secretary-General's 2015 Plan of Action to Prevent Violent Extremism addresses 'Strategic communications, the Internet and social media'.

In response to such calls, the Global Internet Forum to Counter Terrorism was established in June 2017 to prevent the use of online platforms by terrorists and violent extremists.[30] The Forum is an industry-led partnership between the Security Council's Counter-Terrorism Executive Directorate (established under resolution 1373 (2001)), the ICT4Peace Initiative,[31] and Tech Against Terrorism,[32] and involves global companies such as Facebook, Microsoft, Twitter, YouTube and Google.

After the Christchurch attacks in 2019, New Zealand led the 'Christchurch Call to Action' to eliminate terrorist and violent extremist content online,[33] initially adopted by 17 States, the

---

22 UN Security Council resolution 2331 (20 December 2016) [7].
23 UN Security Council resolution 2322 (12 December 2016) [12].
24 UN Security Council resolution 1540 (28 April 2004) [2].
25 UN Security Council resolution 1624 (14 September 2005), [1(a)].
26 EU Directive 2017/541 of 15 March 2017 on Combating Terrorism (replacing EU Council Framework Decision 2002/475/JHA and amending EU Council Decision 2005/671/JHA), art 5.
27 Ibid. art 21.
28 Ibid. preamble [11].
29 UN Security Council resolution 2396 (21 December 2017), preamble.
30 https://gifct.org/about.
31 https://ict4peace.org/about-us/mission.
32 https://www.techagainstterrorism.org.
33 Adopted 16 May 2019 https://assets.documentcloud.org/documents/6004545/Christchurch-Call.pdf.

EU Commission, and eight major technology companies. It calls for both the development of industry standards or voluntary frameworks, as well as regulatory or policy measures consistent with internet freedom and human rights law.

B. Related but Legally Distinct Cyber Harms: Cyber-Crime

Working out what comes within the ambit of cyber 'terrorism' also depends on situating it within the spectrum of other 'cyber' harms, from cyber 'crime' to cyber 'attack', and their associated legal regimes. For instance, much discussion has focused on whether a cyber-attack may constitute a prohibited intervention, use of force (under art 2(4) of the UN Charter) or an armed attack (under art 51 of the Charter) under the international law on the use of force, including for the purpose of a State exercising self-defence against, on the territory of, another State.[34] There are related debates about the lawfulness of cyber weapons or means or methods of warfare under international humanitarian law.[35]

Most importantly, certain regional instruments[36] and many national laws already address the wider category of cyber-crime, which, according to UNODC, can encompass the commission of crimes either through, or against, computer data or systems.[37] A *cyber-enabled* crime is one *facilitated* by computer networks but which can occur offline (such as fraud, purchase of illicit items, money laundering, or stalking). A *cyber-dependent* crime involves, for instance, the use of malware code against a computer network target (such as a 'denial of service' or ransomware attacks).

Cyber-terrorism intended to harm people or property, and intimidate populations or compel a government, can be distinguished from ordinary cybercrime. This includes malicious 'hacking' (such as theft of information, industrial espionage, defacing of websites or 'denial of service' attacks, distribution of 'malware', 'ransomware', phishing emails); political or social 'hacktivism'; and the use of the internet to facilitate terrorism.

More progress has been made at the regional level in addressing cyber-crime than at the international level. The Council of Europe's Convention on Cybercrime 2001 has been

---

[34] See e.g., Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 *Journal of Conflict and Security Law* 211; Nicholas Tsagourias, 'Cyber-attacks, Self-Defence and The Problem of Attribution' (2012) 17 *Journal of Conflict and Security Law* 229; Johann-Christoph Woltag, 'Cyber Warfare' (2015) *Max Planck Encyclopedia of Public International Law*, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e280?prd=EPIL. For further discussion of the application of the *jus ad bellum* to cyber-attacks see Part III of this Handbook.

[35] See e.g., Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017); Michael N Schmitt, 'Classification of Cyber Conflict' (2012) 17 *Journal of Conflict and Security* Law 245; Yoram Dinstein, 'The Principle of Distinction and Cyber War in International Armed Conflicts' (2012) 17 *Journal of Conflict and Security Law* 261; David Turns, 'Cyber Warfare and the Notion of Direct Participation in Hostilities' (2012) 17 *Journal of Conflict and Security Law* 279. For further discussion of the application of IHL to cyberspace see Part IV of this Handbook

[36] See e.g., Council of Europe Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004, CETS No 185); EU Directive 2013/40/EU of 12 August 2013 on Attacks against Information Systems (replacing EU Council Framework Decision 2005/222/JHA). On the international legal dimensions of cyber crime see Kastner and Mégret (Ch 12 of this Handbook).

[37] UNODC, *Draft Comprehensive Study on Cybercrime* (2013), 12. See also Hamid Jahankhani, Ameer Al-Nemrat and Amin Hosseinian-Far, 'Cybercrime Classification and Characteristics' in Akhgar et al (n 6) 149.

ratified or acceded to by 63 States, including most Council of Europe members and various non-member States (including the US and Japan). It criminalizes a range of computer-related offences (which could also be committed by terrorists), including illegal access, illegal interception, data interference, system interference, misuse of devices, forgery, fraud and child pornography.[38]

Notably, the Council of Europe's Committee of Experts on Terrorism has opined that no 'gaps exist' between the Cybercrime Convention and the Council's Convention on the Prevention of Terrorism.[39] It accordingly suggested that the focus should be on the effective implementation of those conventions, rather than instigating 'new negotiations [which] might jeopardize [the existing conventions'] increasing impact on the international fight against cybercrime and terrorism.'[40] The Committee did suggest, however, that increased sanctions may be appropriate in cases involving terrorist attacks against computer systems.[41]

The European Union similarly adopted a Directive on Attacks against Information Systems in 2013, which highlights 'increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure' of States, as well as how gaps and differences in national laws impede the suppression of such attacks.[42] It simply establishes offences of illegal access, illegal system interference, illegal data interference, and illegal interception.[43]

General offences of cyber-crime may go a long way towards obviating the need for a more specific cyber-terrorism offences. Indeed, cyber-crime offences may substantially cover the field of cyber-terrorism, unless there are policy reasons (discussed below) for differentiating between different types of cyber harms and creating more tailored offences – for example, to recognize that cyber-terrorism involves additional elements of intimidation or compulsion.

There is as yet no international treaty on cyber-crime. However, the UN Convention against Transnational Organized Crime 2000[44] enables transnational criminal cooperation in relation to serious crimes under national law (meaning those punishable by at least four years' imprisonment) where the offence is transnational[45] and an organized group is involved. Such groups must be structured, involve three or more people, exist for a period of time, and aim to commit serious crimes to obtain a financial or other material benefit (art 2(a)).

In general, terrorism is often distinguishable from 'ordinary' transnational organized crime for private profit because of the political or other 'public' motive underlying terrorism. But it depends on how terrorism is defined; while some national laws include a political motive

---

[38] Council of Europe Convention on Cybercrime 2001 (n 36) arts 2–9 respectively.

[39] Committee of Experts on Terrorism (CODEXTER), Opinion for the Attention of the Committee of Ministers on Cyberterrorism and the Use of Internet for Terrorist Purposes (2008) 2.

[40] Ibid., 3.

[41] Ibid., 2.

[42] EU Directive 2013/40/EU of 12 August 2013 on Attacks against Information Systems (n 36) preamble [3], see also [27].

[43] Ibid. arts 3–6 respectively.

[44] UN Convention against Transnational Organized Crime (adopted 15 November 2000, entered into force 29 September 2013, 2225 UNTS 209).

[45] An offence is transnational where it is committed in more than one State; or a substantial part of it is prepared, planned, directed or controlled in another State; or it is committed in one State but the criminal group has activities elsewhere, or the crime has substantial effects elsewhere: art 3.

element,[46] many more do not.[47] It can thus overlap with the category of organized crime, particularly given the structured and organized characteristics of many terrorist groups. More importantly, even terrorist groups with political motives may still act for profit in certain contexts, particularly if a narrow view is taken of the immediate intention behind their fundraising activities (whether robbing banks, extorting businesses, or trafficking drugs).

3. 'SECTORAL' INTERNATIONAL ANTI-TERRORISM CONVENTIONS

As already noted, cyber-terrorism has not been specifically prohibited or criminalized at the international level. Some acts of cyber-terrorism may nonetheless be covered by existing terrorism related conventions. Numerous 'sectoral' treaties on transnational criminal cooperation, adopted since the 1960s, target the common methods of violence used by terrorists (such as hijacking, hostage taking, endangering maritime facilities and so on),[48] but do not

---

[46] As in the UK, Canada, Australia, South Africa and New Zealand: see Ben Saul, 'The Curious Element of Motive in Definitions of Terrorism: Essential Ingredient or Criminalizing Thought?' in Andrew Lynch, Edwina MacDonald, and George Williams (eds), *Law and Liberty in the War on Terror* (Federation Press 2007) 28.

[47] See the numerous national laws cited in UN Special Tribunal for Lebanon (Appeals Chamber), *Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging*, STL-11-01/I, 16 February 2011, [106].

[48] Convention on Offences and Certain Other Acts Committed on Board Aircraft (adopted 14 September 1963, entered into force 4 December 1969) 704 UNTS 219 ('Tokyo Convention 1963'); Convention for the Suppression of Unlawful Seizure of Aircraft (adopted 16 December 1970, entered into force 14 October 1971) 860 UNTS 105 ('Hague Convention 1970'); Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation 1971 (adopted 23 September 1971, entered into force 26 January 1973) 974 UNTS 178 ('Montreal Convention 1971'); Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (adopted 14 December 1973, entered into force 20 February 1977) 1035 UNTS 167 ('Protected Persons Convention 1973'); International Convention against the Taking of Hostages (adopted 17 December 1979, entered into force 3 June 1983) 1316 UNTS 205 ('Hostages Convention 1979'); Convention on the Physical Protection of Nuclear Material (adopted 3 March 1980, entered into force 8 February 1987) 1456 UNTS 101 ('Vienna Convention 1980'); Protocol on the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (adopted 24 February 1988, entered into force 6 August 1989) 974 UNTS 177 ('Montreal Protocol 1988'); Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (adopted 10 March 1988, entered into force 1 March 1992) 1678 UNTS 221 ('Rome Convention 1988'); Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf (adopted 10 March 1988, entered into force 1 March 1992) 1678 UNTS 304 ('Rome Protocol 1988'); Convention on the Marking of Plastic Explosives for the Purpose of Detection (adopted 1 March 1991, entered into force 21 June 1998) 2122 UNTS 359 ('Plastic Explosives Convention 1991'); International Convention for the Suppression of Terrorist Bombings (adopted 15 December 1997, entered into force 23 May 2001) 2149 UNTS 256 (Terrorist Bombings Convention 1997); Terrorist Financing Convention 1999 (adopted 9 December 1999, entered into force 10 April 2002) 2178 UNTS 107; Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation 1988 (adopted 14 October 2005, entered into force 28 July 2010) ('Protocol 2005 to the Rome Convention 1988') (UNTS); Protocol 2005 to the Rome Protocol 1988 (adopted 14 October 2005, entered into force 28 July 2010) ('Protocol 2005 to the Rome Protocol 1988'); Amendment to the Convention on the Physical Protection of Nuclear Material 1980 (adopted 8 July 2005, not yet in force); International Convention for the Suppression of Acts of Nuclear

create a new international crime of terrorism.[49] Such treaties typically require States parties to criminalize certain conduct, establish extraterritorial jurisdiction over it, and cooperate by prosecuting or extraditing suspected offenders.

This pragmatic, functional approach enabled the repression of common terrorist methods while side-stepping the irreconcilable problem of defining 'terrorism', especially during the Cold War when States were unable to agree on the legitimacy of violence by self-determination movements or State forces. Such an approach was necessary because it was the only achievable one at the time. This is not, however, an entirely satisfactory means of regulating the criminal aspects of terrorism.

Because the sectoral treaties were adopted in an ad hoc and reactive fashion, they do not comprehensively suppress all possible terrorist methods, or even the most commonly used ones, and they do not protect all conceivable civilian objects. The treaties only criminalize violence by terrorists in specific contexts or by particular methods, and thus fail to prohibit the terrorist killings of civilians by *any* means or method. Just as there is no treaty addressing terrorist acts by use of small arms, biological or chemical toxins, or against public infrastructure or places, there is no treaty on cyber-terrorism. This is despite the great importance of computer networks and electronic infrastructure to the working of modern economies and societies. The negotiation of new treaties is typically stimulated by the occurrence of a major attack utilizing the means in question. A serious cyber terrorist attack may thus be the stimulus necessary for political interest and legal action.

It is unlikely that the drafters of most of the sectoral treaties anticipated the threat of cyber-terrorism, some of which were drafted before the spread of the internet. Most of the treaty offences are squarely aimed at physical attacks on protected targets or by prohibited means. Some of the more recent conventions, however, are more conscious of cyber threats.

A. Aviation and Maritime Safety

Some of the offences in the aviation and maritime safety conventions are broad enough to encompass at least some cyber-attacks, particularly where offences are defined by the harm resulting and contemplate any, rather than only specified, means. The first instrument, the Tokyo Convention 1963, applies to offences under national law concerning acts, by persons on board an aircraft in flight, which 'jeopardize the safety of persons or property therein or which jeopardize good order and discipline on board' (art1). The Convention could conceivably apply to a passenger using a phone or computer to interfere with flight controls or navigation.

The same goes for the hijacking offence under the Hague Convention 1970, which applies to any person on board an aircraft in flight who, by force, threat of force, or intimidation,

---

Terrorism (adopted 13 April 2005, entered into force 7 July 2007) ('Nuclear Terrorism Convention 2005') 2445 UNTS 89; Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation 2005 (adopted 14 October 2005, entered into force 28 July 2010) (UNTS); Convention on the Suppression of Unlawful Acts relating to International Civil Aviation 2010 (adopted 10 September 2010, entered into force 1 July 2018) ('Beijing Convention 2010'); Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft, done at Beijing (adopted 10 September 2010, entered into force 1 January 2018) ('Beijing Protocol 2010'); Protocol to Amend the Convention on Offences and Certain Other Acts Committed on Board Aircraft (adopted 4 April 2014, not yet in force) ('Montreal Protocol 2014').

[49] See Ben Saul, *Defining Terrorism in International Law* (OUP 2006) ch 3.

seizes, or exercises control of, the aircraft (art 1). A threat to take 'control' over the aircraft by cyber means is possible, depending on technological capabilities, albeit presently unlikely. The Beijing Protocol 2010 expands the hijacking offence to include seizure or control also by 'coercion' as well as by 'any technological means' (art 2), implying that cyber methods are definitely contemplated, such as jamming of air navigation[50] or electronic systems. As importantly, the Protocol deletes the Hague Convention's requirement of a perpetrator being 'on board', thereby encompassing external perpetrators, who are more likely than a passenger to be able to operate, without disruption, the cyber equipment to necessary to perform the sophisticated act of remote seizure or control of an aircraft.

Some offences under the Hague Convention 1971 may also extend to cyber acts. For instance, it is an offence to damage or interfere with air navigational facilities if it is likely to endanger the safe flight of an aircraft.[51] Air navigation facilities include physical objects on the ground or on an aircraft,[52] including, for example, signal or air control towers, radio devices, meteorological services,[53] radars, transmitters, and transponders. They also include, as the Beijing Convention 2010 amending the Hague Convention 1971 clarifies, 'signals, data, information or systems necessary for the navigation of the aircraft' (art 2(c)). Consequently, it is an offence to 'damage or interfere with', by physical or cyber means, the physical infrastructure or intangible data of air navigation. Examples of non-kinetic methods could include interference in radio, radar, electronic or computer systems, such as by radio or radar jamming, or other analogue, electronic, digital, or cyber means.

The Hague Convention 1971 also makes it an offence to communicate false information if that is likely to endanger flight safety.[54] Again, this could be occasioned by internet-based communications technologies, such as sending a false signal to divert or land an aircraft.[55] Similar offences to those in the Hague Convention 1971 exist in relation to the safe navigation of ships under the Maritime Safety Convention 1988;[56] an example could be remotely altering a vessel's GPS navigation system.[57]

There are further sectoral treaty offences of placing 'by any means whatsoever' a device or substance on an aircraft, ship or fixed platform, where it is likely to endanger its safety.[58] Likewise, it is an offence to use 'any device, substance or weapon'[59] to destroy or seriously damage the facilities, or disrupt the service of, an airport.

There is an interpretive question whether cyber interference (such as through a computer virus, worm, or 'Trojan horse'), may qualify as 'placing' a dangerous 'device' or 'substance' on an aircraft, ship or platform; or likewise whether it constitutes using 'device, substance

---

[50] Alejandro Piera and Michael Gill, 'Will the New ICAO-Beijing Instruments Build a Chinese Wall for International Aviation Security?' (2014) 47 *Vanderbilt Journal of Transnational Law* 145, 169.

[51] Montreal Convention 1971, art 1(d).

[52] Commonwealth Secretariat, 'Implementation Kits for the International Counter-Terrorism Conventions' (Commonwealth Secretariat 2003) 78.

[53] Ruwantissa Abeyratne, *Aviation Security Law* (Springer Verlag 2010) 240.

[54] Montreal Convention 1971, art 1(e).

[55] Commonwealth Secretariat (n 52) 78.

[56] Rome Convention 1988, art 3(e) and (f) respectively.

[57] Kriangsak Kittichaisaree, *Public International Law of Cyberspace* (Springer 2017) 312.

[58] Respectively, Montreal Convention 1971, art 1(c); Rome Convention 1988, art 3(d); Rome Protocol 1988, art 2(1)(d).

[59] Montreal Protocol 1988, art 2.

or weapon' against an airport. Those concepts were drafted with more conventional kinetic threats in mind, such as explosives or chemical or biological materials, but they could arguably be more expansively interpreted in the light of contemporary cyber threats.

Some offences in the sectoral treaties are, however, unlikely to cover cyber acts which do not result in kinetic harm to aircraft, airports, ships or maritime platforms. Such offences require an element of physical attack, described in such terms as 'violence' against a person on an aircraft, ship or fixed maritime platform;[60] 'destroying' or 'damaging' an aircraft, ship or fixed platform;[61] seizing or controlling an aircraft (but only by a person on board), ship or fixed platform by 'force', threat of force, or 'intimidation';[62] or injuring or killing a person in relation to these kinds of acts.[63]

B. Diplomats and Hostages

The Internationally Protected Persons Convention 1973 prohibits certain physical attacks against diplomats (such as murder, kidnapping or other violence), or other 'violent attack' on the person or their liberty, premises, accommodation or transport which endangers their person or liberty.[64] Its emphasis is thus on physical attack. Still, it is possible in rare cases that a 'violent attack' could be perpetrated by, for instance, cyber interference with flight controls or radar systems guiding an aircraft carrying such a person; or by with the computerized controls of a car (such as locks, airbags, navigation, speed, braking and so on).[65]

Cyber-attacks are even less likely to fall within the strictly physical conduct covered by the Hostages Convention 1979, which makes it an offence to seize or detain and threaten to harm a person to compel a third party to do or abstain from doing any act. The threat to harm the hostage in order to compel another person could, however, be communicated online and thus provide evidence of an offence. Terrorist groups involved in kidnapping for ransom, or to make political demands, have often used such tactics, including videos by Islamic State.

C. Terrorist Bombings

Under the Terrorist Bombings Convention 1997, it is an offence to deliver, place, discharge or detonate an 'explosive or other lethal device' in a public place, government facility, on public transport, or in an infrastructure facility, with the intent to cause death or serious injury or extensive destruction resulting in major economic loss.[66] Cyber acts are clearly not explosives, though explosives can of course be detonated remotely by electronic means. A 'cyber' element

---

[60] Respectively, Montreal Convention 1971, art 1(a); Rome Convention 1988, art 3(b); Rome Protocol 1988, art 2(1)(b).

[61] Respectively, Montreal Convention 1971, art1(b); Rome Convention 1988, art 3(c); Rome Protocol 1988, art 2(1)(c).

[62] Respectively, Hague Convention 1970, art 1(a); Rome Convention 1988, art 3(a); Rome Protocol 1988, art 2(1)(a).

[63] Respectively, Rome Convention 1988, art 3(g); Rome Protocol 1988, art 2(1)(g).

[64] Internationally Protected Persons Convention 1973, art 2. Protected persons include Heads of State or government, ministers and diplomats.

[65] Kittichaisaree (n 57) 309.

[66] Terrorist Bombings Convention 1997, art 2(1).

could thus form part of the factual or evidential matrix, without being a legal element of the offence as such.

An 'other lethal device' is defined as one designed or capable of causing death, serious injury or substantial material damage through the release, dissemination or impact of toxic chemicals, biological agents or toxins, radiation, or similar substances. That definition is plainly restricted to certain dangerous physical objects and does not extend to cyber means alone, absent the presence of an explosive or lethal object; a computer cannot kill a person.

D. Nuclear Terrorism

The Convention on the Physical Protection of Nuclear Material 1979 criminalizes unlawful dealings with nuclear material that cause serious harm to people or property, or involve theft, embezzlement, or intimidation (art 7(1)). Again, cyber methods could be used to achieve such results, for instance by hacking control systems to 'disperse' nuclear material;[67] or by issuing an online 'demand' involve a 'threat… of force' or other 'intimidation'.[68] A 2005 Amendment to the Convention creates a further offence against nuclear facilities of sabotage by 'any deliberate act',[69] which again could extend to cyber interference with control systems.

The Convention on Acts of Nuclear Terrorism 2005 further prohibits the use or damage of a nuclear facility in a manner which releases, or risks the release of, radioactive material.[70] Such use or damage could conceivably arise by cyber means. The 'Stuxnet' computer worm attack on Iranian uranium enrichment centrifuges in 2010, allegedly by the US and Israel, is a case in point, although no radiation was released, or at risk of release, in that incident. Regardless, it is evident that cyber damage to nuclear facilities (whether reactors, enrichment installations, or storage depots), that risks release of radiation, is possible in principle.

A rare reference to cyber technology is found in the Beijing Convention 2010 on aviation safety, which consolidates and modernizes the Montreal Convention 1971 and Montreal Protocol 1988. It creates an offence of the unauthorized transport on a civil aircraft 'any equipment, materials or software or related technology that significantly contributes to the design, manufacture or delivery of a BCN [biological, chemical or nuclear] weapon'.[71] It thus explicitly recognizes that data may be an indispensable ingredient of such weapons.

4. CYBER ACTS UNDER AN INTERNATIONAL CRIME OF TERRORISM

In part because of a desire to comprehensively plug these gaps in the transnational repression of terrorist violence, the international community has continued to feel compelled to pursue a more general transnational crime of terrorism. The long-running saga of international attempts to define and criminalize terrorism, from the 1930s to the present, is well known.[72]

---

67 Vienna Convention 1980, art 7(1)(a).
68 Ibid., art 7(1)(d).
69 Amendment 2005 to the Nuclear Material Convention 1979, art 2A(1)(c).
70 Nuclear Terrorism Convention 2005, art 2(1)(b).
71 Beijing Convention 2010, art 1(1)(i)(4).
72 See Saul (n 49).

The UN Draft Comprehensive Anti-Terrorism Convention, under negotiation under the auspices of the General Assembly since 2000, reflects the widest contemporary international consensus on the issue, albeit subject to a few lingering disagreements. The adoption of the Draft Convention and its general definition of terrorist offences would go a long way towards criminalising most instances of cyber-terrorism, plugging the gaps in the pastiche of sectoral conventions, and largely obviating the need for a cyber-terrorism-specific convention.

A. The Definition of Terrorist Offences

Article 2(1) of the Draft Convention proposes an offence of terrorism if a person 'unlawfully and intentionally' and 'by any means' causes: '[d]eath or serious bodily injury to any person'; '[s]erious damage to public or private property'; or '[d]amage to property, places, facilities, or systems… resulting or likely to result in major economic loss'.[73] The purpose of such conduct, 'by its nature or context', must be 'to intimidate a population, or to compel a Government or an international organization to do or abstain from doing any act'.[74]

This definition of terrorist offences would cover most instances of cyber-terrorism without being too overbroad or under-inclusive. Unlike the approach in the sectoral treaties, it is not limited to the stipulation of specific terrorist methods but explicitly covers 'any means' by which the prohibited harms may be committed. The use of cyber *means* to harm people, seriously damage property, or cause major economic loss by damaging property is thus an offence. The purported customary international law crime of transnational terrorism, recognized by the UN Special Tribunal for Lebanon in 2011, similarly encompasses any means of committing terrorism,[75] although the existing of a customary crime remains much doubted.[76] In this respect the Draft Convention diverges from UN Security Council resolution 1566 (2004), which limits the Council's (non-binding) conception of terrorism to acts which are already offences under the sectoral treaties.[77]

---

[73] UNGA (56thSession) (6th Committee), Measures to Eliminate International Terrorism: Working Group Report, 29 October 2001, A/C.6/56/L.9, annex I, 16 (informal Coordinator texts).

[74] Ancillary offences are found in UN Draft Comprehensive Terrorism Convention, art 2(2), (3) and (4)(a)–(c).

[75] UN Special Tribunal for Lebanon (Appeals Chamber) (n 47) [85]:

> (i) the perpetration of a criminal act (such as murder, kidnapping, hostage-taking, arson, and so on), or threatening such an act; (ii) the intent to spread fear among the population (which would generally entail the creation of public danger) or directly or indirectly coerce a national or international authority to take some action, or to refrain from taking it; (iii) when the act involves a transnational element.

See also *R v Mohammed Gul* [2012] EWCA Crim 280.

[76] Ben Saul, 'Legislating from A Radical Hague: The UN Special Tribunal for Lebanon Invents an International Crime of Transnational Terrorism' (2011) 24 *Leiden Journal of International Law* 677; Kai Ambos, 'Judicial Creativity at the Special Tribunal for Lebanon: Is There a Crime of Terrorism under International Law?' (2011) 24 *Leiden Journal of International Law* 655; Stefan Kirsch and Anna Oehmichen, 'Judges Gone Astray: The Fabrication of Terrorism as an International Crime by the Special Tribunal for Lebanon' (2001) 1 *Durham Law Review* 32.

[77] UN Security Council resolution 1566 (8 October 2004), [3]:

> criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an

The Draft Convention definition could thus include, for instance, cyber-attacks against computer systems which control critical public infrastructure such as transport networks (air, rail, road or sea), water and sewage, or energy supplies (such as electricity or gas distribution networks). But it would also encompass cyber-attacks causing serious harm to private property, such as the deletion or manipulation of economic information relating to banking, stock holdings and the like.

In addition, the definition explicitly safeguards certain cyber or cyber-related objects which may be the target of terrorist attacks (whether by physical or cyber means). Under Article 2(1), 'property' expressly includes 'a place of public use, a State or government facility, a public transportation system, an infrastructure facility... or the environment'.[78] In turn an 'infrastructure facility' is defined in Article 1(3) to include 'communications, telecommunications and information networks'.

Thus an act which causes 'serious damage' (whether temporary or permanent) to a public or private computer, communications or other electronic systems, whether public or private, is a terrorist offence, whether the damage is inflicted by conventional physical means (such as setting on fire a building containing computer servers) or computer-based interference (such as planting a destructive virus). Such an act is an offence even if the serious damage to a computer system does not have the further effect of damaging any 'real world' property or objects which some computer systems are capable of controlling.

The definition in the Draft Convention does, however, contain a number of necessary limitations. Acts must cause death or personal injury, 'serious' property damage, or 'major economic loss'. While the parameters of 'serious' property damage are somewhat slippery, it indicates that minor damage caused by cyber-attacks is excluded. It is right that cyber-attacks that merely 'disrupt nonessential services or that are mainly a costly nuisance' ought to be treated as cyber-crime rather than terrorism.[79] A former UN Special Rapporteur on Terrorism and Human Rights emphasized that the label of cyber-terrorism should be reserved for acts intended to cause 'disruption or destruction sufficient enough to terrorize the population'.[80]

Thus 'hacktivists' who engage in 'electronic civil disobedience',[81] such as the global group Anonymous, would not usually cause sufficient harm to life or property to be classified as committing terrorist acts. Common hacktivist operations include taking control of and defacing websites; distributing computer worms or viruses; overloading a server with external communications requests to prevent it processing legitimate internet traffic (a 'denial of service attack'); or using automated programs to bombard a target with thousands of emails (an 'email bomb').[82] Such acts may not constitute cyber-terrorism even if the perpetrators are regarded as

---

international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism.

78 UN Draft Comprehensive Terrorism Convention, art 2(1)(b).

79 Dorothy Denning, 'Cyberterrorism' (Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives, 23 May 2000).

80 Kalliopi Koufa, Special Rapporteur on Terrorism and Human Rights, 'Progress Report' (27 June 2001) E/CN.4/Sub.2/2001/31, 28 [101].

81 Dorothy Denning, 'Activistm, Hactivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy' in John Arquilla and David Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime and Militancy* (RAND 2001) 263.

82 Ibid., 263–80.

terrorist groups, as where resistance movements such as Hezbollah and Hamas have allegedly hacked various Israeli government and commercial websites.[83]

It remains possible, however, that such activities cause serious economic harm, such as where corporate websites are disabled resulting in the loss of revenue. An example is Anonymous' 'Operation Avenge Assange', which targeted payment entities (such as Paypal and credit card companies) which had bowed to US pressure to refuse to process donations to Wikileaks.[84] Such attacks were instrumentally designed to coerce corporate and government behaviour. Such acts would not usually, however, be regarded as 'terrorism' in the popular consciousness, illustrating the potential overreach of the Draft Convention definition.

Even hacking techniques used by terrorist groups will not amount to cyber-terrorism where they do not cause serious damage to persons or property. One example of the use of these techniques by a terrorist group involved the Liberation Tigers of Tamil Eelam (LTTE) sending around 800 emails a day to Sri Lankan embassies around the world in 1997.[85] The emails read 'We are the Internet Black Tigers and we're doing this to disrupt your communications'. Embassy networks were disabled for two weeks. Although sending a strong and intimidatory political message, such disruption should not be considered an act of cyber-terrorism, since it did not harm people or 'seriously' damage property. However, if a similar attack disrupted a critical service, such as emergency medical communications,[86] resulting in serious harm, liability for terrorism could be appropriate.

For similar reasons, State-sponsored cyber-attacks which do not cause serious harm also fall outside the ambit of the Draft Convention offences. One example is attacks on western government and corporate websites by the Syrian Electronic Army (aligned with the Assad regime in Syria).[87] Another example is the activities of PLA Unit 61398, a Chinese government military unit which has launched cyber-attacks on foreign governments and companies.

A further important limitation in the Draft Convention's definition of terrorism is that the purpose of an act must be 'to intimidate a population, or to compel a Government or an international organization to do or abstain from doing any act'. A similar 'special intent' element is found in the UN Security Council's guideline definition of terrorism in resolution 1566 (2004) and in the purported customary international law crime of transnational terrorism recognised by the UN Special Tribunal for Lebanon in 2011.[88] The Security Council definition suggests a third alternative intent element, 'the purpose to provoke a state of terror in the general public or in a group of persons or particular persons',[89] though that standard is not so different from the other element of intimidating a population.

Cyber-attacks which do not specifically intend to intimidate a population or compel a government or international organization will therefore not qualify as terrorism under the Draft Convention. To some extent this excludes acts which are privately motivated or narrowly

---

[83] Cohen (n 6) 167.

[84] Mark Townsend et al, 'WikiLeaks backlash: The First Global Cyber War has Begun, Claim Hackers' *Guardian* (Online, 12 December 2010) www.theguardian.com/media/2010/dec/11/wikileaks-backlash-cyber-war.

[85] See Yvonne Jewkes and Majid Yar, *Handbook of Internet Crime* (Routledge 2013) 198–9.

[86] An example provided by Koufa (n 80) [101].

[87] 'Microsoft in more hacking misery', *BBC News* (21 January 2014) www.bbc.co.uk/news/technology-25825781; Cohen (n 6) 167.

[88] UN Special Tribunal for Lebanon (Appeals Chamber) (n 47) [85].

[89] UN Security Council resolution 1566 (8 October 2004) [3].

targeted, although it is still possible for perpetrators motivated by private ends (such as money or revenge, rather than political aspirations) to intimidate populations or coerce governments. (An example might be hacktivists who extort money from a government or corporation in exchange for ceasing to damage public or private property respectively.)

The Draft Convention also does not require proof of a political, religious or ideological motive underlying acts designed to intimidate a population or compel a government. As such, its definition is broader and captures wider conduct as terrorism than common law crimes of terrorism which also require a political motive.[90]

There are also various hard cases where the definition in the Draft Convention would likely classify a cyber-attack as terrorism but the act in question may not be commonly perceived as terrorism by a democratic public. One example is where air traffic controllers, in the midst of an industrial dispute, changed the passwords on their air traffic control computers, to prevent outside workers performing their jobs.[91] Such conduct is plainly dangerous to aircraft and passengers, and was done to coerce the government in labour negotiations. But many would be instinctively uneasy about classifying industrial protest, even dangerous or excessive strike activity, as 'terrorism'.

Another example is where an anti-coal mining activist issued a fake press release (using a laptop and mobile phone in a forest), purportedly from a major bank, announcing that the bank had withdrawn its funding for a major mine development. The mining company's share value on the stock market rapidly dropped by A$314 million, before recovering after the hoax was exposed.[92] The hoaxer's conduct could conceivably be characterized as terrorism under the Draft Convention: using cyber means to cause serious private property damage and/or major economic loss, arguably intended (in part) to compel the government to revoke its approval of the coal mine.[93] Yet, such an act of environmental protest is far from regarded as 'terrorist' in the popular imagination, even if it may transgress ordinary domestic criminal law. The hoaxer was actually charged with making a false and misleading statement under domestic corporations' law.[94]

The above example illustrates the difficulty that even an apparently tightly drafted definition of terrorism – limited to serious harms committed for prohibited instrumental purposes – is still likely to capture some non-terrorist conduct. It suggests that good sense is needed in the selection of charges in the exercise of prosecutorial discretion – an obvious point, but one necessary to reiterate in a world where too many national authorities abuse their legal systems to settle political scores. It may further demonstrate that a 'carve out' provision for democratic protest or dissent, which does not cause personal injury, should be tacked on to the

---

[90] Saul (n 46).

[91] Committee on Freedom of Association, Case No 1913 (Panama), Report No 309 (March 1998) 112.

[92] 'Environmentalist's Hoax Triggers $314m Whitehaven Share Price Fall', *Sydney Morning Herald* (8 January 2013).

[93] The hoaxer asserted that civil disobedience was necessary because the community was locked out of the approval process and there are fewer legitimate avenues to protect the environment: 'Anti-coal Activist Jonathan Moylan Granted Bail Over Whitehaven Share Hoax', *ABC News* (23 July 2013).

[94] Leo Shanahan, 'Jonathan Moylan's Whitehaven Hoax Case to Go to the Supreme Court', *The Australian* (24 September 2013).

definition of terrorism in the Draft Convention, just as Australia has done in its federal offence of terrorism.[95]

B. Exclusions from a General Crime of Cyber-Terrorism

While the definition of terrorism in the Draft Convention was settled reasonably quickly, stimulated by the attacks of 9/11, disagreement remains over its scope of application to certain non-State and State violence.[96] Those disagreements are also relevant to regulation of cyber-terrorism. Presently the Draft Convention excludes from its scope the activities of State and non-State armed forces in armed conflict covered by international humanitarian law[97] (even if debate remains about which groups come within the meaning of armed forces).

Thus, cyber-attacks by armed forces (including 'terrorist' groups such as Islamic State) in armed conflict cannot be characterized as cyber-terrorism. That does not mean that such forces are free to attack civilians by cyber means or to destroy cyber targets. The usual rules of international humanitarian law apply, including the principles of distinction and proportionality and the prohibition on causing superfluous injury or unnecessary suffering. Most terrorist-type conduct committed in an armed conflict is prohibited.[98] It is therefore appropriate that the *lex specialis*, humanitarian law, governs the cyber activities of armed forces in armed conflict, and little substantive would be gained by also addressing such acts under the Draft Convention.

In addition, any act or threat thereof, the primary purpose of which is to spread terror among the civilian population, is already prohibited by the laws of war.[99] The influential (albeit unofficial) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* concludes that this could include a cyber-attack.[100] A breach of this IHL prohibition amounts to the war crime of spreading terror amongst a civilian population.[101] This war crime is defined by the special intent of the perpetrator to spread terror beyond the ordinary incidental fear often felt by civilians living through conflict.

There are, however, some critical uncertainties as to the extent to which IHL protects against cyber operations. IHL prohibits 'attacks' (defined as 'acts of violence') against civilian 'objects'.[102] An attack is conventionally interpreted to include violent acts (such as kinetic

---

[95] Criminal Code Act 1995 (Australia), s 100.1(3).

[96] See UNGA (57th Session) (6th Committee), Measures to Eliminate International Terrorism: Working Group Report, UN Doc A/C.6/57/L.9, annex II (16 October 2002) 7–8. Little headway was made between 2003 and the present (2019).

[97] UN Draft Comprehensive Terrorism Convention, art 20(2).

[98] Hans-Peter Gasser, 'Acts of Terror, "Terrorism" and International Humanitarian Law' (2002) 84 *International Review of the Red Cross* 547.

[99] This is based on art 51(2) of Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (adopted on 8 June 1977, entered into force 7 December 1978, 1125 UNTS 3) and art 13(2) of Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts (adopted on 8 June 1977, entered into force 7 December 1978, 1125 UNTS 609).

[100] Tallinn Manual 2.0 (n 35) Rule 98.

[101] *Prosecutor v Galic*, ICTY-98-29-T (5 December 2003), [65-66]; affirmed in *Prosecutor v Galic (Appeals Chamber Judgment)*, IT-98-29-A (30 November 2006), [87-90]. See also Ben Saul, 'Crimes and Prohibitions of "Terror" and "Terrorism" in Armed Conflict: 1919-2005' (2005) 4 *Journal of the International Law of Peace and Armed Conflict* 264.

[102] Additional Protocol I of 1977, arts 49(1) and 52(1) respectively.

force) as well as violent consequences (such as injury to people or damage property); while objects are conventionally understood as 'visible and tangible' things (including computer hardware), but excluding data.[103] It is broadly accepted that a cyber operation can be an attack under IHL if it foreseeably results in injury or death to persons or damage or destruction of objects[104] – that is, it has kinetic or 'real-world' harmful effects.

In addition, there is wide support for the view that an operation against data which affects the functionality of physical objects can constitute an attack, at least where restoring functionality requires replacement of physical components (such as where the control system or vital components of an electrical grid must be replaced).[105] Mere disruption of email services, even on a national scale, would not, however, qualify, nor would cyber espionage, jamming, or inconvenience to civilian internet usage.[106]

The real controversy resides in targeting data alone, without there being any wider kinetic or violent (injurious or damaging) effects. According to the majority of experts involved in the *Tallinn Manual 2.0*, data of itself is intangible and therefore not an 'object' regulated by IHL.[107] As such, it may be targeted, since it is not an object regulated by IHL. This means that not only military data (including malware weapons or personnel records) can be targeted, but also civilian data – such as social security or tax information, bank accounts, business records, or election lists. In contrast, a minority of *Tallinn Manual 2.0* experts, plus the ICRC, argue for a wider interpretation of a protected 'object' to encompass at least that data which is essential to the well-being of the civilian population, given the severity, not the nature, of the resulting harm.[108]

If the majority view prevails, the exclusion of cyber operations of armed forces from the Draft Convention is problematic, since neither it nor IHL prohibits attacks on civilian data. There is then a strong case for the Draft Convention to criminalize at least those cyber operations that have the specific intent of intimidating or compelling. There is also a good argument that the deletion or modification of data essential to civilian well-being should also be established as a sectoral-treaty type offence, that is, even where it is not intended to intimidate or compel, given the serious consequences for civilians that it entails.

Equally problematic is the further proposed exclusion under the Draft Convention of the activities of State armed forces in the exercise of their official duties in peace time.[109] Numerous examples of offensive State cyber-attacks with a 'terrorist' quality can be contemplated: crashing the computer systems of a foreign central bank, stock market, or commodities exchange; shutting down oil pipelines carrying heating fuel for civilians in winter; sabotaging an air traffic control system; or remotely interfering in a dangerous manufacturing process, thereby endangering workers or causing property damage. Mention was made earlier of the activities of a Chinese military hacking unit; various other States, such as the United States, also have offensive cyber-attack capabilities.

---

[103] Tallinn Manual 2.0 (n 35) Rule 92 [3] and Rule 100 [5-6] respectively.
[104] Ibid., Rule 92 [6] and Rule 100 [6].
[105] Ibid., Rule 92 [10].
[106] Ibid., Rule 92 [13-14].
[107] Ibid., Rule 100 [6].
[108] Ibid., Rule 100 [7].
[109] UN Draft Comprehensive Terrorism Convention, art 20(3).

It is true that cyber-attacks by State militaries outside an armed conflict may be covered by the international prohibition on the use of force, the principle of non-intervention, and international human rights law (including in its extraterritorial dimension). But it does not follow there also exists individual criminal liability for illegal cyber-attacks by State military forces, whether against foreign States (military or civilian) or private persons. Only in limited circumstances is there liability for the crime of aggression (due to the grave scale of the attack), while a crime against humanity may only be committed if there is a widespread or systematic attack on a civilian population.

In other, perhaps less intense circumstances, however, State militaries would be exempt from international criminal liability for cyber-attacks on other States or populations in peace time, even where they cause personal injury or property damage (and are not justified under the international law of self-defence). Admittedly, criminal liability will be borne under the Draft Convention by other (non-military) State officials or agents, including law enforcement officials and security or intelligence services. But that makes it all the more strange that the same legal responsibility is not borne by State military personnel under the Convention, when it is difficult to see any principled or pragmatic need to award them such an exemption.

5. REGIONAL INSTRUMENTS

Similar to the UN Draft Comprehensive Convention, it should also be briefly mentioned that some cyber-attacks are likely to come within the wide general definitions of terrorist offences in certain regional counter-terrorism instruments, which often focus on the harmful consequences rather than the means used. In EU law, for example, these could include the terrorist offences of 'release of dangerous substances, or causing fires, floods or explosions, the effect of which is to endanger human life', or 'interfering with or disrupting the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life'.[110] Under African Union law, it is a terrorist offence to 'disrupt any public service, [or] the delivery of any essential service' in certain circumstances.[111]

EU law explicitly recognizes certain acts of cyber-terrorism as terrorist offences. First, there is a terrorist offence of 'causing extensive destruction to… an information facility… likely to endanger human life or result in major economic loss',[112] where such conduct also meets the specific intent elements of a terrorism offence.[113] The offence thus captures cyber-terrorism that causes physical harm as well as more intangible (albeit very serious) economic harm.

Second, it is a terrorist offence where an illegal system interference, or illegal data interference (both as defined by *renvoi* to these concepts in arts 4 and 5 of EU Directive 2013/40 on Attacks against Information Systems, mentioned above) involves the special intent elements

---

[110] EU Directive 2017/541 of 15 March 2017 on Combating Terrorism (n 26) art 3(1)(g) and (h).

[111] Organisation of African Unity (OAU) Convention on the Prevention and Combating of Terrorism (adopted 14 July 1999, entered into force 6 December 2002, 2219 UNTS 179), art 1(3)(a)(ii).

[112] EU Directive 2017/541 of 15 March 2017 on Combating Terrorism (n 26) art 3(1)(d).

[113] Namely that it (1) may seriously damage a country or international organization and (2) aims to seriously intimidate a population, unduly compel a government or international organization, or seriously destabilizes or destroys the fundamental political, constitutional, economic or social structures of a country or an international organization.

of terrorism.[114] In addition to the terrorist intent elements, the system and date interference offences have to satisfy further gravity thresholds to constitute terrorism, indicating that the EU is reluctant to classify ordinary interferences as terrorism. Thus, an illegal system interference[115] must (i) affect a significant number of information systems through the use of a tool[116] designed or adapted primarily for that purpose; or (ii) cause serious damage; or (iii) be committed against a critical infrastructure information system. An illegal data interference (which must not be minor)[117] must be committed against a 'critical infrastructure information system'.

The ASEAN Convention on Counter Terrorism 2007 is the only regional instrument to refer to 'cyber-terrorism' as such. Article 6 lists measures to 'strengthen capability and readiness to deal with… cyber-terrorism and any new forms of terrorism' as an 'area of cooperation' between the parties.[118] However, it does not define an offence of cyber-terrorism, and defines 'terrorism' restrictively by reference to the international sectoral treaties.[119]

6. IS THERE A NEED FOR A CYBER-TERRORISM TREATY?

The above review of existing legal frameworks on terrorism generally demonstrates that there is no lacuna in international law that leaves cyber-terrorism completely unregulated or unpunished. Some cyber-terrorism comes within some of the sectoral treaties. The proposed Draft Comprehensive Anti-Terrorism Convention, if adopted, would cover most instances of cyber-terrorism, while many regional instruments also directly or indirectly cover elements of cyber-terrorism.

Further, much cyber-terrorism can also be classified as cyber-crime under some regional (and many national) laws, and sometimes under the Convention against Transnational Organized Crime, though there is as yet no international treaty on cyber-crime per se. Other international norms, including binding Security Council measures, deal extensively with acts facilitative of terrorism generally, which cover cyber activities.

In addition, at a more abstract level, all States bear a long-standing, international obligation to diligently prevent and repress terrorist activities emanating from their territory and directed towards harming other States.[120] Such obligation is not limited to any particular ter-

---

[114] EU Directive 2017/541 of 15 March 2017 on Combating Terrorism (n 26) art 3(1)(i).

[115] Defined in EU Directive 2013/40/EU of 12 August 2013 on Attacks against Information Systems (n 36) art 4 as 'seriously hindering or interrupting the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible, intentionally and without right'.

[116] Such as a computer program, password, access code or similar data to access an information system: ibid., art 7.

[117] Ibid., art 5 as 'deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor'.

[118] Association of South East Asian Nations (ASEAN) Convention on Counter Terrorism (adopted 13 January 2007, entered into force 27 May 2011), art 6(1)(j).

[119] Ibid., art 2.

[120] UN General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, annexed to UN General Assembly resolution 2625 (XXV) (1970), [2] (non-intervention), [8-9] (non-use of force); reiterated in numerous General Assembly resolutions on terrorism: 3034 (XXVII) (1972); 32/147 (1977),

rorist means or methods, but extends to any acts capable of causing terrorist harm, including cyber-terrorism. Here difficulty lies not with the normative standards so much as the practical questions of obtaining evidence, proof of State responsibility, and securing effective forum.

A. Sequencing

A question remains whether international law should nonetheless respond more pointedly or precisely to cyber-terrorism, rather than relying upon the incomplete jigsaw of sectoral and general anti-terrorism norms and the fragmented efforts to cooperate on cyber-crime as a whole. The answer is partly one of sequencing. If the Draft Comprehensive Convention can be soon adopted, much of the argument for a separate cyber-terrorism agreement is deflated. The very point of a comprehensive instrument is to capture all forms of terrorism, and to overcome the unsatisfactory ad hoc and partial approach of the sectoral treaties.

If the Draft Convention remains in stasis, however, there are stronger reasons for a cyber-terrorism treaty. Likewise, if there remains no instrument on cyber-crime generally, there is a stronger case for a cyber-terrorism specific instrument to combat that narrow type of it. The issue is partly which instrument will be developed first to plug the same normative gaps.

B. Threat Analysis

The necessity of pursuing a cyber-terrorism instrument partly depends also on extra-legal policy considerations about the gravity and likelihood of the threat. Opinion is divided over whether terrorist groups have the capacity or motivation to commit cyber-terrorism.[121] To date, there have been no confirmed reports of a cyber-terrorism attack. Two UN reports concur that 'there is not yet an obvious terrorist threat in the area' of cyberspace,[122] and that there are 'few indications of terrorist attempts to compromise or disable [Information Communications Technology (ICT)] infrastructure or to execute operations using ICTs'.[123] Thus far there has been far more concern about States launching cyber-attacks on each other (such as Russia's attacks on Estonia in 2007,[124] or Georgia in 2008) than non-State cyber-attacks against States, principally because of the level of technical resources, skills and sophistication often necessary to mount serious and sustained cyber-attacks.

---

preamble; 34/145 (1979), preamble, [7]; 38/130 (1983), [4]; 40/61 (1985), [6]; 42/159 (1987), [4], [5(a)]; 44/29 (1989), [3], [4(a)]; 46/51 (1991), [3], [4(a)]; 49/60 (1994), [4], [5(a)]; 51/210 (1996), [5]; 52/165 (1997), [5]; 53/108 (1999), [5]; 54/110 (2000), [5]; 55/158 (2001), [5]; 56/88 (2002), [5]; 57/27 (2003), [5]; 58/81 (2004), [5]; UNGA (60th Session), World Summit Outcome, UN Doc A/60/L.1 (20 September 2005), [86].

[121] See Denning (n 79).

[122] CTITF (n 3) [92].

[123] Group of Governmental Experts on Developments in the Field of information and Telecommunications in the Context of International Security: Note by the Secretary General, A/65/201 (30 July 2010).

[124] See e.g., Eneken Tikk and Reet Oorn, 'Legal and Policy Evaluation: International Coordination of Prosecution and Prevention of Cyber Terrorism' in Centre of Excellence Defence against Terrorism (ed), *Responses to Cyber Terrorism* (IOS Press 2008) 89, 93–102.

However, some security analysts and policy makers regard the threat of cyber-terrorism as real and likely to intensify. Former US President Obama described 'the cyber threat to our nation' as 'one of the most serious… national security challenges we face',[125] and warned that 'Al Qaeda and other terrorist groups have spoken of their desire to unleash a cyber-attack' on the US.[126] The UK classed a 'cyber-attack, including by… terrorists' as one of four 'Tier One' threats in its National Security Strategy.[127] Israeli Prime Minister Benjamin Netanyahu has accused Hezbollah and Hamas of launching cyber-attacks against Israeli infrastructure.[128] The question is whether these concerns are shared widely enough in the international community to impel enough States to believe it is worthwhile to draft yet another sectoral anti-terrorism treaty, when many are exhausted by the Draft Convention negotiations and implementation of the 19 existing sectoral treaties and protocols.

C. Model National Laws and National Laws

Model cyber-crime legislation promoted by the International Telecommunication Union (ITU) encourages States to more specifically criminalize cyber-terrorism where an underlying cyber-crime is committed 'with the intent of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism'.[129] The model law hinges on national definitions of terrorism. The ITU explains that '[c]ybercrimes… for the purposes of terrorism were deemed to be such a threat to the rule of law, public safety, and national and economic security that the *Toolkit* Project Team believed separate provisions should address these crimes and more substantial penalties should apply'.[130]

At present, however, very few national laws treat cyber-terrorism as a distinct legal offence, whether because States do not view it as sufficiently threatening, ordinary terrorism or cyber-crime laws are considered adequate, or domestic laws have simply been slow to adapt. One rare exception concerns two offences under Indian law since 2008, both carrying a penalty of life imprisonment. The first consists of denying access to a computer resource, accessing a computer resource without authorization, or contaminating a computer, where the specific intent elements of terrorism are also met.[131]

In sum, those intent elements are twofold. First, the conduct must cause death, injury, property damage, damage or disruption of essential supplies or services, or an adverse effect

---

[125] US President Barack Obama, 'Taking the Cyberattack Threat Serious', *Wall Street Journal* (19 July 2012).

[126] US President Barack Obama, 'Remarks by the President on Securing our Nation's Cyber Infrastructure' (Speech, 29 May 2009) www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

[127] UK Government, 'A Strong Britain in an Age of Uncertainty: The National Security Strategy' (Paper presented to Parliament, October 2010), 11. The remaining threats were international terrorism, international military crises between States, and a major accident or national hazard.

[128] Shlomo Cesana and Ilan Gattegno, 'Netanyahu: Iran, Hamas stepping up cyberwarfare against Israel', *Israel Hayom* (10 June 2013).

[129] ITU Toolkit for Cybercrime Legislation (February 2010), ss 2(d), 3(f), 4(f), 6(h). The ITU is a unique UN treaty organisation, as its members include not only 193 States, but also 700 private ICT companies.

[130] Ibid., 32.

[131] Information Technology Act 2000 (India), s 66F(A) (inserted by The Information Technology (Amendment) Act 2008 (India)).

on critical information infrastructure (meaning a computer resource, the incapacitation or destruction of which would have debilitating impact on national security, economy, public health or safety[132]). Second, the conduct must be committed 'with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people'.

A second Indian cyber-terrorism offence involves penetrating or accessing a computer resource without authorization and thereby obtaining access to one of two types of restricted information. The first type is information, data or databases that are restricted for reasons of the security of the State or foreign relations. The second type is any other restricted information, data or database which could injure:

> the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise.[133]

Problematically from the standpoint of human rights and the principle of legality, the Indian law is not limited to cyber acts which are genuinely terrorist. Instead, it labels as a cyber terrorism any person who accesses restricted information through a computer, if that information is likely to cause harms such as damaging friendly relations with foreign States, or injuring public order, decency or morality.[134] Punishment can extend to life imprisonment.

It is more common for general terrorism offences to embed certain cyber acts within their definitional elements, as under the EU terrorism offences mentioned earlier. Thus serious interference, disruption or destruction of electronic systems is an alternative element of general terrorism offences in Australia, the UK, and South Africa[135] (all of which also involve specific intent elements). The Australian and South African laws extensively define 'electronic system' to include information, telecommunications, or financial systems, and systems used for essential government services, essential public utilities, or transport.

In the US, a federal crime of terrorism can be committed where certain predicate computer crimes also satisfy the special intent requirements for terrorism (namely, that the act is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct).[136] Three computer crimes are listed. The first involves unauthorized access to a computer, and consequent unauthorized disclosure, of restricted

---

[132] Ibid., s 70(1).

[133] Ibid., s 66F(B).

[134] Ibid., s 66F(1).

[135] Criminal Code Act 1995 (Australia), s 100.1 (an electronic system is defined as including information, telecommunications, or financial systems, and systems used for essential government services, an essential public utility, or a transport system); Terrorism Act 2000 (UK), s 1(2)(e) (serious interference or serious disruption of an electronic system); Protection of Constitutional Democracy against Terrorism and Related Activities Act 2004 (South Africa), s 1. New Zealand law more obliquely refers to 'serious interference with, or serious disruption to, an infrastructure facility, if likely to endanger human life': Terrorism Suppression Act 2002 (NZ), s 5(3)(d). Canadian law likewise refers to 'serious interference with or serious disruption of an essential service, facility or system, whether public or private': Criminal Code, RSC 1985 c C-46 (Canada), s 83.01(1).

[136] 18 US Code § 2332b(1) and (5).

national defence of foreign relations information so obtained (and which could be used to injure the US or advantage another country).[137]

The second predicate crime involves damaging a protected computer[138] by transmitting a program, information, code, or command, or by accessing a protected computer without authorization.[139] In addition, such acts must cause the further harm of modifying or impairing medical treatment; physical injury; a threat to public health or safety; damaging a US government computer used for the administration of justice, national defence, or national security; or damage ten or more protected computers within one year.[140] The third predicate crime involves injuring or destroying certain US communications systems, interfering in their working, or obstructing, hindering, or delaying their transmissions.[141]

D. Addressing Technical Challenges

One reason for creating a cyber-terrorism specific convention is to address unique technical difficulties that may demand special measures of prevention and repression. There may be '"computer-specific" gaps in "terrorist-specific" conventions'.[142] Examples of necessary technical measures include retention of Internet Service Provider (ISP) or other internet related data,[143] international standards on encryption,[144] the collection and use of electronic evidence in courts,[145] the relationship between State security organizations and private companies who offer cyber services.[146] Traditional mutual legal assistance may also be too slow and cumbersome to effectively and expeditiously secure access to fast-moving online evidence.[147] There are peculiar jurisdiction difficulties in investigating and taking enforcement action in relation to cyber offences, aspects of which may take place across internet servers in multiple countries, or using anonymous methods.

These technical challenges are, however, common to both cyber-crime and cyber-terrorism and are not unique to the latter. As such, alone they do not provide a compelling reason to generate a narrow convention on cyber-terrorism as distinct from a wider, more encompassing instrument on cyber-crime. It is possible that a negotiating a cyber-terrorism instrument could

---

[137] 18 US Code § 1030(a)(1).

[138] Meaning a computer exclusively used by the US government computer or a financial institution, or which affects interstate or foreign commerce or communication: 18 USC § 1030(e)(2).

[139] 18 US Code § 1030(a)(5)(A).

[140] 18 US Code § 1030(c)(4)(A)(i)(II)-(VI).

[141] 18 US Code § 1362.

[142] CODEXTER (n 39) 2.

[143] UNODC (n 4) 92.

[144] Kelly Gable, 'Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent' (2010) 43 *Vanderbilt Journal of Transnational Law* 57, 97.

[145] UNODC (n 4) [365]ff.

[146] CTITF (n 3) 7.

[147] See generally UNODC, CTED and International Association of Prosecutors, *Practical Guide for Requesting Electronic Evidence Across Borders* (2019); Council of Europe, Cybercrime Convention Committee, T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime, 3 December 2014; Council of Europe, Cybercrime Convention Committee, T-CY Guidance Note #10: Production Orders for Subscriber Information (Article 18 Budapest Convention), 1 March 2017; Suleyman Ozeren, 'Cyberterrorism and International Cooperation: General Overview of the Available Mechanisms to Facilitate an Overwhelming Task' in Centre of Excellence Defence against Terrorism (n 124) 70.

lessen the impetus to agree a wider cyber-crime convention, though conversely agreeing a narrower instrument on terrorism could build confidence towards a wider crime convention.

E. Stigmatization

Another reason to pursue a special instrument against cyber-terrorism is to send an expressive or stigmatizing signal that the international community regards it as wrongful. While cyber-terrorism can often already be qualified as ordinary crime or terrorism, a special instrument could more pointedly condemn and punish the abuse of the internet to commit terrorism, possibly strengthening deterrence and encouraging stronger international cooperation. Such an instrument could also potentially address cyber acts facilitative of terrorism, such as the misuse of the internet for incitement, recruitment, financing and the like (even though these are already addressed by separate international standards). There may be effectiveness gains in consolidating and finessing relevant standards in one place, which may outweigh the conceptual messiness of duplicating international efforts across multiple instruments. This presupposes, however, that the threat of cyber-terrorism justifies singling it out for special treatment, and currently there is far from international consensus on that point.

F. Facilitating Transnational Cooperation

A final reason for concluding a convention on cyber-terrorism is to promote consistency between domestic legal regimes and encourage restraint by national governments when determining the scope of cyber-terrorism offences. Mutual assistance, extradition and prosecution of transnational cyber terrorist offences is most feasible and effective where States broadly agree on the underlying definition of cyber-terrorism offences. As noted earlier, currently there are widely divergent national approaches to dealing with the problem, inhibiting the potential for cooperation. At the same time, the lack of an international consensus encourages individual States to potentially adopt over-broad and rights-abusive definitions of cyber-terrorism, a problem arising in the field of terrorism laws generally.

Some States have thus been wary of deepening cooperation on cyber-terrorism for fear that it could lead to the erosion of human rights. The internet is a 'powerful vehicle for the exercise and protection of human rights of freedom of opinion and expression'.[148] International legislative overreach could have a chilling effect on the way that people exercise their rights of opinion and expression over the internet, and can be readily exploited by governments to target political activists or dissidents, and unjustifiably infringe on personal privacy. As mass surveillance controversies in the US and UK suggest, democracies as well as authoritarian States have been tempted by excessive counter-terrorism responses.

6. CONCLUSION

Cyber-terrorism is rarely treated as a discrete legal problem, partly because the threat thus far has been modest, and partly because other legal responses, particularly treating it as

[148] CTITF (n 3) 23.

cyber-crime, cover most pertinent threats. A number of sectoral counter-terrorism convention offences can also be applied to some, but not all, cyber threats; and those conventions are, any event, confined to certain areas, such as aviation and maritime safety, diplomats and hostages, bombings and nuclear terrorism. The Security Council obligations on States to criminalize and suppress financing and other forms of support for terrorism are also capable of capturing the many uses of the internet to facilitate terrorism that stop short of being actual terrorist acts. Some regional and national laws go further in specifically regulating cyber-terrorist methods.

In principle, the risk of cyber-terrorism, albeit still in its infancy, is worthy of suppression. If adopted, the Draft Comprehensive Convention would likely cover most forms of cyber-terrorism, since it focuses more on the harm caused than the specific means used. Normatively there would then be little need for a more specific cyber-terrorism instrument. There may, however, still be a need to develop further cooperation on the technical aspects of investigating, collecting evidence on, and prosecuting such clandestine, technically complex, multi-jurisdictional crimes, while complying with fundamental human rights obligations.

11. Cyber espionage and international law

Russell Buchan and Iñaki Navarrete

1. INTRODUCTION

Cyberspace represents the 'fifth domain' of human activity and it has rapidly emerged as an indispensable feature of modern life.[1] Nowadays, all actors within the international system rely upon cyberspace to conduct their activities and maximise their potential. At the same time, cyberspace can be 'used for purposes that are inconsistent with international peace and security'.[2] Indeed, the threat landscape in cyberspace is multifaceted and dynamic, ranging from hacktivism, cyber vandalism, cyber terrorism to cyber war. In recent years, the exploitation of cyberspace for the purpose of espionage has emerged as a particular concern, with reports suggesting that 'cyber espionage projects [are] now prevalent'.[3]

The scale and intensity of cyber espionage in the contemporary world order was thrust firmly into the international spotlight in 2013 when Edward Snowden – a former contractor for the United States (US) National Security Agency (NSA) – disclosed thousands of classified documents to the British newspaper *The Guardian*.[4] These documents revealed to the world the full extent of the NSA's surveillance efforts. In particular, the NSA had been engaged in a sustained and widespread campaign of collecting confidential information that was being stored in or transmitted through cyberspace. These cyber espionage operations targeted a wide array of State and non-State actors, including officials of international organisations (such as the European Union), State organs (including Heads of State such as German Chancellor Angela Merkel and Israeli Prime Minister Ehud Olmert), religious leaders (the Pope), companies (such as the Brazilian oil company Petrobras), non-governmental organisations (including Médecins du Monde), and individuals suspected of being involved in international terrorism.[5]

---

[1] Netherlands Ministry of Defence, *The Defence Cyber Strategy* (2012) 4, https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/Netherlands_2012_NDL-Cyber_StrategyEng.pdf accessed 9 December 2020.

[2] UN Secretary-General, *Foreword*, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98 (24 June 2013) 6.

[3] Pete Warren, 'State-sponsored Cyber Espionage Projects Now Prevalent', *The Guardian* (30 August 2012) http://www.theguardian.com/technology/2012/aug/30/state-sponsored-cyber-espionage-prevalent accessed 9 December 2020. See also Mandiant Report, *APT1: Exposing one of China's Cyber Espionage Units* (2013) http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf accessed 9 December 2020.

[4] Ewen Macaskill and Gabriel Dance, 'NSA Files: Decoded: What the Revelations Mean For You', *The Guardian* (1 November 2013) https://www.theguardian.com/us-news/the-nsa-files accessed 9 December 2020.

[5] See generally Ed Pilkington, 'Tim Berners-Lee: Spies' Cracking of the Encryption Undermines the Web', *The Guardian* (3 December 2013) http://www.theguardian.com/technology/2013/dec/03/tim-berners-lee-spies-cracking-encryption-web-snowden accessed 9 December 2020.

Incidents such as these raise several important and novel questions concerning the legality of cyber espionage under international law.[6] With this in mind, the objective of this chapter is to broach how international law applies to cyber espionage. Section 2 provides a working definition of cyber espionage in order to frame this chapter's research scope. This section also makes it clear that the focus of this chapter is on the application of international law to 'political' and 'economic' cyber espionage. Section 3 situates political and economic cyber espionage within its broader international political context and examines the impact of this conduct on the maintenance of international peace and security. Section 4 analyses the application of the principle of territorial sovereignty to political and economic cyber espionage. Section 5 assesses whether the law of the World Trade Organization regulates economic cyber espionage. Section 6 offers conclusions.

2. DEFINING CYBER ESPIONAGE

Espionage has been a fixture of international relations 'since the dawn of human history'[7] and one commentator wryly refers to it as the world's 'second oldest profession'.[8] In its traditional conception, espionage describes the dispatch of State agents into the territory of other States in order to obtain confidential information. Yet, States have exploited technological developments to devise more effective techniques for conducting espionage. With the invention of ships, aeroplanes and satellites, the sea, the sky and outer space have emerged as spaces from which to conduct espionage. It therefore comes as no surprise that, since its inception, cyberspace has also been exploited for the purpose of espionage. In fact, cyberspace represents 'God's gift to spies' and there are several reasons for this.[9] First, cyberspace is used to store and transmit large volumes of confidential information, thus making it a resource-rich environment in which spies can operate. Second, as an anonymous domain, cyberspace enables spies to access confidential information with little chance of being identified. Third, even if the identity of a cyber spy is uncovered, cyber espionage can be committed remotely and beyond the jurisdictional reach of the target State, thereby making it a relatively risk-free activity.

'Espionage' is a descriptive term rather than an international legal concept,[10] and it has failed to attract an internationally recognised definition.[11] Rather than attempt to produce

---

[6] For a review of the international law literature on cyber espionage see Russell Buchan and Iñaki Navarrete, *Cyber Espionage* (2020) *Oxford Bibliographies*, https://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0212.xml accessed 9 December 2020.

[7] Katharina Ziolkowski, 'Peacetime Cyber Espionage – New Tendencies in Public International Law' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (CCDCOE 2013) 425.

[8] Michael J Barrett, 'Honorable Espionage' (1984) 2 *Journal of Defence and Diplomacy* 13, 14.

[9] James Lewis, Senior Vice President at the Centre for Strategic and International Studies, quoted in David P Fidler, 'Tinker, Tailor, Soldier, Duqu: Why Cyberespionage is More Dangerous than You Think' (2012) 5 *International Journal of Critical Infrastructure Protection* 28, 29.

[10] '"Spying" is a colloquial, rather than a legal, term'; Craig Forcese, 'Spies Without Borders: International Law and Intelligence Collection' (2011) 5 *Journal of National and Security Law and Policy* 179, 181.

[11] '[There is no] internationally recognized and workable definition of "intelligence collection"'; Glenn Sulmasy and John Yoo, 'Counterintuitive: Intelligence Operations and International Law' (2006) 28 *Michigan Journal of International Law* 625, 637.

a formal definition of cyber espionage – which would be a difficult and perhaps even futile task – time is better spent identifying this activity's most prominent features.

1. The essence of espionage is the *non-consensual* collection of confidential information.[12] Information accessed with the owner's consent does not therefore constitute espionage – for example, where treaties permit States parties to access each other's confidential information.[13] Critically, cyber espionage involves more than mere hacking into a computer system or network that stores confidential information. To qualify as cyber espionage, electronic data must be *copied*.[14] Moreover, cyber espionage occurs regardless of whether data is damaged or deleted. Thus, targets may never know that they have fallen victim to cyber espionage and, indeed, this is usually when espionage is at its most effective.
2. Espionage takes different forms depending upon the actors involved as well as the nature of the information targeted and a loose 'typology' of espionage has emerged.[15] 'Political' espionage involves States stealing confidential information from other States and is designed to shed light on their capabilities and intentions. 'Economic' espionage is also State-sponsored and describes the theft of confidential business information from foreign companies, usually with the intention of passing it to domestic companies. Non-State actors also engage in espionage.[16] In this context, 'industrial' espionage (sometimes referred to as 'commercial' espionage) involves companies stealing trade secrets from foreign companies without the support or assistance of a State. This chapter examines the legality of espionage conducted by States, that is, *political* and *economic* espionage.[17]
3. More specifically, this chapter is concerned with political and economic espionage committed in *cyberspace*. Cyberspace refers to a 'global domain within which the information environment consisting of the interdependent network of information technology infrastructure, including the Internet, telecommunications networks, computer systems,

---

[12] '[I]ntelligence analysis that relies on open source information is legally unproblematic'; Simon Chesterman, 'The Spy Who Came in From the Cold War: Intelligence and International Law' (2006) 27 *Michigan Journal of International Law* 1071, 1073.

[13] For instance, the Treaty on Open Skies 1992. See also art 20 (Consent), International Law Commission, *Articles on State Responsibility for Internationally Wrongful Acts* (2001).

[14] Ziolkowski (n 7) 429. For a criticism of this definitional feature see Leah West, 'Book Review: *Cyber Espionage and International Law* by Russell Buchan' (2019) 56 *Canadian Yearbook of International Law* 634, arguing that this definition fails to encapsulate the copying of information that is not intended to be resident in, or transiting through, cyberspace but may be captured remotely using a target's cyber-connected hardware, for instance by surreptitiously taking photographs of a room using a computer's webcam.

[15] See e.g. Craig Forcese, 'Spies without Borders: International Law and Intelligence Collection' (2011) 5 *Journal of National Security Law and Policy* 179, 181.

[16] 'A growing array of state and non-state adversaries are increasingly targeting – for exploitation and potentially disruption or destruction – our information infrastructure including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical infrastructure'; Director of National Intelligence Dennis C Blair, *Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee*, Statement for the Record (February 2009) 39–40.

[17] For an analysis of the application of international law to industrial espionage, see Russell Buchan, 'Taking Care of Business: Industrial Espionage and International Law' (2019) 26 *Brown Journal of World Affairs* 143.

and embedded processors and controllers'.[18] Cyber-enabled espionage can take the form of 'close' or 'remote' access. Close access cyber espionage is where the perpetrator operates in close proximity to the targeted information, for instance, where a spy physically enters the territory of the target State and downloads information onto a memory stick. By contrast, remote access cyber espionage is performed at some distance from the targeted information, usually exploiting pathways created by the Internet.[19]

4. The focus of this chapter is on the legality of political and economic cyber espionage under *international* law. Certainly, cyber espionage can violate a State's internal (and usually criminal) law.[20] However, with regard to remote access cyber espionage at least, States will find it difficult to exercise their jurisdiction over perpetrators located in foreign jurisdictions.[21] The advantage of establishing that cyber espionage breaches international law is that the international legal system allows States to engage in self-help measures when they fall victim to internationally wrongful acts. Notably, international law permits States to take countermeasures to the extent necessary to induce a wrongdoing State into law-compliance and implement State responsibility.[22]
5. Cyber espionage can be committed during times of peace or armed conflict. International law does not regulate peacetime espionage *per se*.[23] Instead, different rules of international law apply to peacetime espionage on the basis of the actors involved, the underlying act and the legal context within which it occurs.[24] By contrast, espionage conducted during times of armed conflict is directly and specifically regulated by international humanitarian law.[25] Due to space restrictions, and given the widespread practice of peacetime cyber

---

[18] Joint Publication (JP) 1, Doctrine for the Armed Forces of the United States, *DOD Dictionary of Military and Associated Terms* (January 2020) 55 https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf accessed 9 December 2020.

[19] Herbert S Lin, 'Offensive Cyber Operations and the Use of Force' (2010) 4 *Journal of National Security Law and Policy* 63, 66.

[20] Spencer Ackerman and Jonathan Kaiman, 'Chinese Military Officials Charged with Stealing US Data as Tensions Escalate', *The Guardian* (20 May 2014) http://www.theguardian.com/technology/2014/may/19/us-chinese-military-officials-cyber-espionage accessed 9 December 2020. For instance, see Security of Information Act (R.S.C., 1985, c. O-5).

[21] In relation to US indictments of Chinese officials for their involvement in economic cyber espionage, Fidler explains that '[t]he U.S. government knows the likelihood of successfully prosecuting these individuals for violating U.S. criminal law is virtually nil because the cooperation of the Chinese government would be necessary for the U.S. to gain custody and conduct a criminal trial'; David P Fidler, 'Cyber Espionage Indictment of Chinese Officials' (19 May 2014) https://archive.news.indiana.edu/releases/iu/2014/05/china-cyber-spying.shtml accessed 9 December 2020.

[22] Articles on State Responsibility for Internationally Wrongful Acts (n 13) arts 49–54.

[23] See Iñaki Navarrete and Russell Buchan, 'Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions' (2019) 51 *Cornell International Law Journal* 897, 901–5.

[24] 'While the International Group of Experts agreed that there is no prohibition of espionage *per se*, they likewise concurred that cyber espionage may be conducted in a manner that violates international law due to the fact that certain methods employed to conduct cyber espionage are unlawful'; Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) 170.

[25] Hague Regulations 1907; Geneva Convention 1949; Additional Protocols to the Geneva Conventions 1977.

espionage in recent years, the focus of this chapter is upon the application of international law to *peacetime* cyber espionage.[26]

3. CYBER ESPIONAGE AND THE MAINTENANCE OF INTERNATIONAL PEACE AND SECURITY

3.1 Political Cyber Espionage

Political espionage is often defended on the basis that it serves an important function in maintaining international peace and security.[27] Generally, this defence is rooted in classic realist theory.[28] Central to this theory is the belief that, because the world order lacks an overarching government that is capable of protecting State security, States inhabit an environment that can be characterised as a Hobbesian state of nature.[29] In the absence of a centralised authority that is capable of protecting States from external threats, States must assume responsibility for their own survival in the system. In practice, this means that States must acquire enough material power to deter potential aggressors from attack and, if necessary, repel them.[30] All in all, international peace and security is maintained where there is a balance of power between States.[31]

Evidently, identifying the relative strengths and weaknesses of other States is critical to achieving a balance of power. In a realist world order, the benefit of espionage is that it allows States to better understand the capabilities and intentions of their adversaries.[32] In this sense, espionage facilitates the achievement of a balance of power and thus plays an important role in maintaining international peace and security.[33] After subscribing to this theoretical framework, scholars maintain that political espionage must be free from international legal regulation.[34]

---

[26] On wartime cyber espionage see Marco Longobardo, '(New) Cyber Exploitation and (Old) International Humanitarian Law' (2017) 77 *Zeitschrift Für Ausländisches öffentliches Recht und Völkerrecht* 809.

[27] See generally Michael Herman, *Intelligence Power in Peace and War* (CUP 1996).

[28] On realism as a theory of international relations see Edward H Carr, *The Twenty Years' Crisis: 1919–1939* (Palgrave Macmillan 1939).

[29] Thomas Hobbes, *Leviathan* (first published 1651, CUP 1904) 81–6.

[30] See generally Kenneth Waltz, *Theory of International Relations* (Addison-Wesley Pub. Co 1979).

[31] '[W]ars usually begin when two nations disagree on their relative strength, and wars usually cease when the fighting nations agree on their relative strength'; Geoffrey Blainey, *The Causes of War* (The Free Press 1988) 293.

[32] 'In an anarchical order, understanding the intentions and capabilities of other actors has always been an important part of statecraft'; Chesterman (n 12) 1076.

[33] 'Espionage is regarded by States as a necessary tool for pursuing their foreign policy and security interests and for maintaining the balance of power at the inter-State level. Thus, it has always been a common practice in international relations, even in time of peace'; Christian Schaller, 'Spies' (2009) *Max Planck Encyclopaedia of Public International Law*. Parks argues that States regard espionage 'as a vital necessity in the national security process'; W Hays Parks, 'The International Law of Intelligence Collection' in John Norton Moore and Robert Turner (eds), *National Security Law* (Carolina Academic Press 1990) 433.

[34] Sulmasy and Yoo claim that the international legal regulation of political espionage 'will likely prove counterproductive to the goal of promoting international peace and security'; Sulmasy and John (n 11) 625.

In an anarchical world order, realists argue that political espionage is also necessary because it enables States to confront the growing threat posed by hostile non-State actors such as terrorist organisations.[35] In particular, realists claim that espionage operations against terrorist groups allow States to acquire a better understanding of the nature of the threat they represent. For example, espionage enables States to identify which individuals are involved in terrorist organisations and to pinpoint with greater accuracy when and where terrorist attacks will occur. Armed with this information, States can develop strategies and implement measures to counteract terrorist threats.[36]

The Achilles heel of this defence of political espionage is that realism no longer provides an accurate account of the nature and structure of contemporary international relations.[37] More to the point, the weakness of realism is that it fails to appreciate that, since at least 1945, States have transformed the anarchic structure of world order into an international society that is predicated upon the respect for mutually agreed principles and values.[38] In the wake of the devastation wrought by the Second World War, States recognised that they possessed a common interest in devising a more effective system for maintaining international peace and security. To this end, the principle of the sovereign equality of States was posited as the foundational (or even constitutional) norm of the international society,[39] and the United Nations was subsequently devised in order to institutionalise – and therefore buttress – this normative framework.[40] At its core, the principle of the sovereign equality of States casts all States *qua* States as juridically equal entities that are entitled to determine their internal affairs free from external interference.[41] In the international society, then, international peace and security is maintained through a recognition of, and respect for, common principles and values rather than through a balance of power.

Even if espionage is effective in allowing States to access useful information relating to their adversaries, it is nevertheless the case that this conduct is at odds with the principle of the sovereign equality of States. States often go to great lengths to keep their information secret: they classify it under national law; keep it under lock and key; store it electronically behind password-protected firewalls; and encrypt digital data. It therefore follows that the theft of a State's confidential information undermines its decision-making capacity and, fundamentally, compromises its sovereign authority.

In fact, this reasoning applies *mutatis mutandis* to espionage operations carried out against non-State actors located within the territory of other States (e.g., against individuals belonging

---

[35] Ibid., 636.

[36] '[Intelligence operations] have prevented multiple [terrorist] attacks and saved innocent lives – not just here in the United States, but around the globe'; President Barack Obama, *Remarks by the President on Review of Signals Intelligence*, 17 January 2014, www.obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signalsintelligence accessed 9 December 2020.

[37] Anne-Marie Slaughter, 'International Law in a World of Liberal States' (1995) 6 *European Journal of International Law* 503.

[38] Russell Buchan, *International Law and the Construction of the Liberal Peace* (Hart 2013) Chapter 1.

[39] Hedley Bull, *The Anarchical Society: A Study of Order in World Politics* (Palgrave 2002) 16–17.

[40] Art 2(1) UN Charter 1945. See generally Bardo Fassbender, 'The United Nations Charter as Constitution of the International Community' (1998) 36 *Columbia Journal of Transnational Law* 529.

[41] Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, Principle C, UN Doc A/RES/25/2625 (24 October 1970).

to terrorist groups). Flowing from the principle of sovereign equality, States exercise sovereign authority over all actors within their jurisdiction.[42] From the perspective of the international society, then, espionage against non-State actors subsumed under the sovereign authority of a State constitutes interference in that State's internal affairs.

More recently, commentators such as Baker have offered functionalism as an alternative justification for espionage.[43] At the heart of the functionalist defence is the recognition that the contemporary international society faces a range of complex threats, including inter-State conflict, human rights violations, environmental degradation, economic insecurity, poverty, health crises, etc. Baker maintains that the international society can only address these threats where its members enjoy close and effective cooperation and are able to conclude international agreements aimed at their resolution. In light of this, he claims that the benefit of espionage is that it allows States to verify whether other States are complying with their international commitments.[44] Baker argues that where States insist that they are meeting their obligations and, through espionage, this is revealed to be true, a sense of trust will emerge between them. On the back of this, he argues that States are more likely to cooperate across functional lines and conclude additional agreements that are designed to resolve common threats.[45] Baker therefore contends that political espionage enhances the maintenance of international peace and security and, for this reason, international law should demonstrate a 'tolerance' for this activity.[46]

Writing in the context of *cyber* political espionage, Pelican likewise explains that '[t]he benefits to international stability and cooperation as outlined by … Baker are as relevant today as they ever have been'.[47] After explicitly adopting Baker's reasoning, Pelican concludes that cyber espionage 'should be recognized as a valuable tool for countries in promoting international stability'[48] and that 'cyber-espionage, like other forms of espionage, should persist unabated'.[49]

This functional defence of espionage is not wholly convincing. On the one hand, we agree with Baker's observation that effective cooperation within the international society is critical to the maintenance of international peace and security. On the other hand, we view the surreptitious, non-consensual collection of confidential information as undermining the international society's core principle on the sovereign equality of States. As such, espionage can breed distrust and hostility rather than foster comity and cooperation. Thus, espionage can sometimes have the opposite effect of that envisaged by Baker and his adherents: espionage can act as a barrier to functional cooperation and thus impede States' efforts to resolve threats to international peace and security.[50]

---

[42] *Island of Palmas* case, 2 RIAA (Perm Ct Arb 1928) 829, 838.

[43] Christopher D Baker, 'Tolerance of International Espionage: A Functional Approach' (2003) 19 *American University International Law Review* 1091.

[44] 'When armed with such tools as spying and eavesdropping, states enjoy greater certainty that they will be able to validate international compliance, or at least detect when other participants are failing to comply with the treaty'; ibid., 1104.

[45] Ibid., 1105

[46] Ibid., 1095.

[47] Luke Pelican, 'Peacetime Cyber-Espionage: A Dangerous But Necessary Game' (2012) 20 *CommLaw Conspectus* 363, 385.

[48] Ibid., 364.

[49] Ibid., 385.

[50] As Fidler explains, espionage is '[far from] harmless. It can create significant costs, disrupt national security strategies, and destabilize relations between nations'; David P Fidler, 'Wither the

A good example of the adverse impact that espionage has on international cooperation is illustrated by the Gary Powers affair. Powers was a pilot of a US spy plane that was shot down while in Soviet Union airspace in May 1960. This incident prompted a marked deterioration in relations between the US and the Soviet Union. Notably, recriminations from both sides meant the much-anticipated Four Powers Peace Summit that was due to take place in Paris on 16 May 1960 ended in failure. In fact, Soviet President Nikita Khrushchev explicitly blamed the US's spying for derailing the talks and subsequently rescinded an invitation he had extended to President Eisenhower to visit the Soviet Union.[51]

Similarly, the disruptive impact that *cyber-enabled* espionage has upon international cooperation was laid bare by the fallout from the Edward Snowden revelations. In particular, these disclosures revealed that the US had routinely conducted cyber espionage operations against Brazil. In response, Brazilian President Dilma Rousseff cancelled a scheduled meeting with the Obama administration in Washington DC to discuss issues affecting regional security in the Americas. Instead, Rousseff proceeded to New York and formally denounced the NSA's activities before the UN General Assembly. In doing so, she explained that cyber espionage impinges on State sovereignty which, in turn, inhibits effective inter-State cooperation: 'Friendly governments and societies that seek to consolidate a truly strategic partnership, such as is our case, cannot possibly allow recurring and illegal actions to go on as if they were normal, ordinary practice. Such actions are totally unacceptable.'[52]

When cast in this light, a compelling normative justification emerges for why international law should constrain the practice of political cyber espionage.

3.2 Economic Cyber Espionage

During the Cold War, States defined their national security principally through the lens of military strength. However, the Soviet Union's demise at the end of the Cold War was attributed at least in part to its failed national economy (rather than its inadequate military capabilities),[53] thereby revealing a close nexus between a State's economic security and its national security.[54]

Critical to a State's economic security is the prosperity of national companies, which create jobs, pay taxes and attract domestic and foreign investment. Recognising this, some States go to great lengths to acquire foreign companies' trade secrets, targeting information relating to product development processes, marketing strategies, customer lists, etc.[55] Once acquired, States pass this information to national companies with the objective of sharpening their com-

---

Web?: International Law, Cybersecurity, and Critical Infrastructure Protection' (Fall 2015) *Georgetown Journal of International Affairs* 8, 12.

[51] '1960: East-West Summit in Tatters After Spy Plane Row', *BBC News* (17 May 1960), http://news.bbc.co.uk/onthisday/hi/dates/stories/may/17/newsid_2512000/2512335.stm accessed 9 December 2020.

[52] Julian Borger, 'Brazilian President: US surveillance a 'breach of international law', *The Guardian* (24 September 2013) http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance accessed 9 December 2020.

[53] See generally Ann J Tickner, 'Re-Visioning Security' in Ken Booth and Steve Smith (eds), *International Relations Theory Today* (Polity Press 1995).

[54] Catherine Lotrionte, 'Countering State-Sponsored Cyber Economic Espionage Under International Law' (2015) 40 *North Carolina Journal of International Law and Commercial Regulation* 443, 444.

[55] Shahar Argaman and Gabi Siboni, 'Commercial and Industrial Cyber Espionage in Israel' (2014) 6 *Military and Strategic Affairs* 43, 46.

petitive edge in the marketplace. With this achieved, national companies are able to contribute to the State's economic security and thus enhance its national security.

Yet, economic espionage harms the economic security of the State that plays host to the target company and it does so in a number of ways. First and foremost, when a company obtains access to another company's trade secrets it can produce similar products at cheaper prices because it does not have to incur research and development costs. Once these products are placed on the open market, the victim company loses the revenue it would have expected to generate and which was intended to cover its research and development costs. Indeed, for some companies the exclusivity of their products is essential to their economic success and, when it is undermined, their continued survival in the market is jeopardised.[56]

Second, trade secret theft inhibits creativity and innovation. The reason for this is because companies are unlikely to pour funds and resources into developing new products if their foreign competitors are able to obtain their trade secrets, replicate their products and market them at cheaper prices.[57] In a nutshell, economic espionage suppresses ambition and reduces profitability.

To give a sense of the problem, the Intellectual Property Commission estimates that China's theft of intellectual property from US companies costs the US economy between $225 billion and $600 billion a year.[58] In response to these figures, the US Office of the Director of National Intelligence concludes that 'the technologies cultivated by American minds and within American universities are at risk of becoming the plunder of competing nations at the expense of long-term US security'.[59] Echoing this view, the United Kingdom maintains that '[economic] [c]yber espionage presents a real risk to the economic well-being of the UK. It poses a direct threat to UK national security'.[60]

Given the adverse impact that economic cyber espionage has on a victim State's national security, it becomes clear that international law should play a central role in regulating this practice.

---

[56] Gabi Siboni and David Israel, 'Cyberspace Espionage and its Effect on Commercial Considerations' (2015) 7 *Military and Strategic Affairs* 39.

[57] Gerald O'Hara, 'Cyber-Espionage: A Growing Threat to the American Economy' (2010) 19 *CommLaw Conspectus* 241.

[58] Intellectual Property Commission, *The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy* (2017) 4, http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf accessed 9 December 2020. See also Council on Foreign Relations, *A New Old Threat: Countering the Return of Chinese Industrial Espionage* (December 2018) https://www.cfr.org/report/threat-chinese-espionage accessed 9 December 2020.

[59] Office of the Director of National Intelligence, *Economic Espionage*, https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-threat-assessments-mission/ncsc-economic-espionage accessed 9 December 2020. 'Foreign economic and industrial espionage against the United States continues to represent a significant threat to America's prosperity, security, and competitive advantage'; National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace* (2018) 4, https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf accessed 9 December 2020.

[60] MI5, *Cyber* (2020) https://www.mi5.gov.uk/cyber accessed 9 December 2020.

4. THE PRINCIPLE OF TERRITORIAL SOVEREIGNTY

One of the most pressing challenges in international law today is that of sovereignty in cyberspace and, in relation to espionage, two central questions surface. The first is whether the principle of territorial sovereignty operates as a primary rule of customary international law imposing an obligation on States not to breach the sovereignty of other States. This issue needs unpacking because of the ongoing 'discord' regarding the existence of sovereignty in cyberspace.[61] If the answer to this question is 'yes', the second – and far more relevant – question is that of the precise threshold at which cyber operations such as remote access cyber espionage breach the rule.

The question of whether a 'customary espionage exception' to the principle of territorial sovereignty exists is distinct and will not be discussed here. That question goes not to the existence of the principle of territorial sovereignty in cyberspace, but simply to the presence of certain exceptions to an otherwise established rule. At any rate, and as we have shown elsewhere,[62] the notion that the practice of espionage has taken on a patina of custom is open to challenge.

4.1 Cause of Action

In recent years, some States and scholars have questioned whether the principle of territorial sovereignty constitutes a *rule* of international law the breach of which gives rise to an independent cause of action. Rather, their argument is that sovereignty is a 'principle' of international relations from which certain rules of international law stem (e.g., non-intervention and the prohibition on the threat or use of force). The signal example of this approach is embodied in the speech of 23 May 2018 of UK Attorney General Jeremy Wright, when he stated that:

> Some have sought to argue for the existence of a cyber specific rule of a 'violation of territorial sovereignty' in relation to interference in the computer networks of another state without its consent. Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law.[63]

The upshot of this view is that cyber operations falling below the threshold of intervention and use of force are permissible, such as is the case with close and remote access cyber espionage. In our view, this is the wrong inquiry. In reality, there can be no doubt that the principle of

---

[61] See Gary P Corn and Robert Taylor, 'Sovereignty in the Age of Cyber' (2017-2018) 111 *American Journal of International Law Unbound* 207; Michael N Schmitt and Liis Vihul, 'Respect for Sovereignty in Cyberspace' (2017) 95 *Texas Law Review* 1639; Sean Watts and Theodore Richard, 'Baseline Territorial Sovereignty and Cyberspace' (2018) 22 *Lewis and Clark Law Review* 771. On sovereignty in cyberspace see generally Tsagourias (Ch 1 of this Handbook).

[62] Navarrete and Buchan (n 23).

[63] Speech of Attorney General Jeremy Wright, *Cyber and International Law in the 21st Century*, 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century accessed 9 December 2020. See also NATO, *Allied Joint Publication 3.20, Allied Joint Doctrine for Cyberspace Operations* (January 2020) v (UK reserving its position on the principle of territorial sovereignty).

territorial sovereignty operates as a stand-alone rule of international law the breach of which constitutes a cause of action recognised by customary international law.

In the international jurisprudence, one of the first manifestations of this can be found in the judgment of the International Court of Justice (ICJ) in the *Corfu Channel* case.[64] In October 1946, two British warships struck mines while passing through Albania's territorial waters. Three weeks later, the UK launched 'Operation Retail', which was a minesweeping operation carried out in Albania's territorial waters and without its consent. The UK argued that Operation Retail was an instance of self-help carried out in order to collect evidence for its international case. The Court did not accept this argument. It noted that '[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations',[65] and held that the UK had breached Albania's sovereignty.

In the 1986 *Nicaragua* case, the ICJ likewise held that the principle of territorial sovereignty constitutes a stand-alone rule of international law, one that can be breached by non-consensual acts conducted on another State's territory such as espionage. Nicaragua complained *inter alia* of infringement of its airspace by US high- and low-altitude spy flights.[66] The Court indicated that the '[t]he principle of respect for territorial sovereignty is … directly infringed by the unauthorized overflight of a State's territory by aircraft belonging to or under the control of another State'.[67] That the principle of territorial sovereignty constitutes a stand-alone rule of international law is made evident not only by the reasoning of the Court but also by the operative clauses of its judgment, which distinguish between the US breaches of the principles of non-use of force and non-intervention, and those breaches involving the principle of territorial sovereignty alone.[68] On this last ground, the Court concluded that, by directing or authorising overflights of Nicaraguan territory, the US had 'acted in breach of its obligations under customary international law not to violate the sovereignty of another State'.[69]

This principle of responsibility for violations of territorial sovereignty is accepted in the practice of States. An extensive review of this practice is unnecessary but, for illustrative purposes, the Savarkar,[70] U-2,[71] Pueblo,[72] Rainbow Warrior,[73] and Cosmos 954[74] incidents all

---

[64] *Corfu Channel* case, Judgment [1949] ICJ Rep 4.

[65] Ibid., 35.

[66] *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment (Merits) [1986] ICJ Rep 14, para 87.

[67] Ibid., para 251.

[68] Ibid., Compare operative clauses (3) (non-intervention), (4) (use of force), and (5) (territorial sovereignty).

[69] Ibid., operative clause (5), 147.

[70] *The Savarkar Case* (Great Britain, France), 24 February 1911, Reports of International Arbitral Awards, volume XI, 243–55.

[71] On this incident see Quincy Wright, 'Legal Aspects of the U-2 Incident' (1960) 54 *American Journal of International Law* 836.

[72] On this incident see Alfred P Rubin, 'The Impact of the Pueblo Incident in International Law' (1969) 49 *Oregon Law Review* 1.

[73] On this incident see Geoffrey Palmer, 'Settlement of International Disputes: The Rainbow Warrior Affair' (1989) 15 *Commonwealth Law Bulletin* 593.

[74] See for instance the Canadian claim against the USSR for the penetration of its territory by the Cosmos 954 satellite: 'The intrusion of the Cosmos 954 satellites into Canada's air space… constitutes a violation of Canada's sovereignty. This violation is established by the mere fact of the trespass of the satellite…'; Claim against the Union of Soviet Socialist Republics for Damage Caused by Soviet Cosmos 954, *International Legal Materials* 18, No. 4 (July 1979): 899–930.

demonstrate that the breach of the obligation to respect territorial sovereignty may constitute an independent cause of action for the injured State.[75]

We therefore reject the contention that the principle of territorial sovereignty does not operate as a rule of international law. That the application of the rule to cyberspace poses special problems is evident. But these sorts of problems are not new, and they have routinely formed part of the makeup of the international debate, with each new space that has opened with scientific advance.

In fact, the UK's position has become increasingly isolated as a number of States have come out in support of territorial sovereignty as an autonomous rule of international law that applies to cyberspace. For example, statements by Finland,[76] France,[77] Germany,[78] Canada,[79] Austria,[80]

---

[75] For a compelling demonstration of the independent status of the principle of territorial sovereignty under international law, see Schmitt and Vihul (n 61).

[76] Finland, *International Law and Cyberspace: Finland's National Position* (2020) 1, 'It is undisputed that the principle of State sovereignty applies in cyberspace … In this sense, sovereignty is a foundational principle of the international legal order' https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859 accessed 9 December 2020.

[77] République Française, Ministère des Armées, *Droit International Appliqué aux Opérations dans le Cyberespace* (2019) 7, https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf accessed 9 December 2020:

> Any cyberattack against French digital systems or any effects produced on French territory by digital means by a State organ, a person or an entity exercising elements of governmental authority or by a person or persons acting on the instructions of or under the direction or control of a State constitutes a breach of sovereignty.

[78] 'Even in cases where one cannot speak of a use of force, the use of cyber capabilities might constitute a violation of sovereignty, if the attack can be attributed to a state, which then in turn could lead to consequences within the confines of public international law'; Norbert Riedel, 'Cyber Security as a Dimension of Security Policy', Speech of Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London on 18 May 2015.

[79] 'Canada identifies malicious cyber-activity by Russia', Statement of Global Affairs Canada dated 4 October 2018 (speaking of the hack of the OPCW and World Anti-Doping Agency and stating that '[t]he incidents identified by Canada and our allies, including the GRU's attempt to undermine the work of the OPCW, underscore the Russian government's disregard for the rules-based international order, international law and established norms') https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html accessed 9 December 2020.

[80] Austria, *Pre-Draft Report of the OEWG – ICT: Comments by Austria* (31 March 2020) https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf accessed 9 December 2020.

Iran,[81] Chile,[82] Bolivia,[83] Guatemala,[84] Guyana,[85] New Zealand[86] and the Czech Republic[87] point to a shared understanding of the applicability of the principle of respect for territorial sovereignty in cyberspace as an autonomous obligation.

Likewise, following close access cyber espionage activities by Russia's GRU targeting the Organisation for the Prohibition of Chemical Weapons' (OPCW) offices in The Hague in 2018, the Netherlands was prompted to publicly provide its view on the application of international law to cyberspace.[88] In one document, it expressed its belief that 'respect for the sovereignty of other countries is an obligation *in its own right*, the violation of which may in turn constitute an internationally wrongful act'.[89]

4.2 Threshold

Having demonstrated that territorial sovereignty is a principle of international law, the immediate task is to unpack its content and identify the threshold for its application in cyberspace. Fundamentally, the principle of territorial sovereignty confers upon States the right to perform governmental functions within their territory without external interference.[90] What constitutes a governmental function depends on the political constitution of each State – in short, States allocate different functions to their governments. However, certain core governmental func-

---

[81] See Statement of the General Staff of Iranian Armed Forces 'General Staff of Iranian Armed Forces Warns of Though Reaction to Any Cyber Threat' (July 2020), 'The sovereignty of states is not an extra-legal matter' https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat accessed 9 December 2020.

[82] For the position of Latin-American States on this issue, see OEA/Ser. Q, CJI/doc. 603/20 rev. 1, 5 March 2020, 'International Law and State Cyber Operations: Improving Transparency', fourth report presented by Dr. Duncan B. Hollis, 19–20, http://www.oas.org/en/sla/iajc/docs/CJI_doc_570-18.pdf accessed 9 December 2020.

[83] Ibid.

[84] Ibid.

[85] Ibid.

[86] New Zealand, *The Application of International Law to State Activity in Cyberspace* (1 December 2020) para 11 https://www.mfat.govt.nz/en/media-and-resources/ministry-statements-and-speeches/cyber-il/ accessed 9 December 2020.

[87] Statement by Mr. Richard Kadlčák, Special Envoy for Cyberspace, Director of Cybersecurity Department, Czech Republic (11 February 2020) 'The Czech Republic concurs with those considering the principle of sovereignty as an independent right and the respect to sovereignty as an independent obligation' https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf accessed 9 December 2020.

[88] Netherlands, *Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace* (July 2019) https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace accessed 9 December 2020. See also the appendix to this letter: *Appendix: International Law in Cyberspace*, file:///Users/russell/Downloads/International+Law+in+the+Cyberdomain+-+Netherlands%20(6).pdf accessed 9 December 2020. See also Michael N Schmitt, 'The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis' (14 October 2019) *Just Security*, https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/ accessed 9 December 2020.

[89] Netherlands, Appendix: International Law in Cyberspace (n 88) 2 (our emphasis).

[90] *Island of Palmas* (n 42) 838; *Nicaragua* (n 66).

tions can be identified. For example, a common function across governments is the right to determine who enters and who leaves State territory.

With regard to a State's physical territory – land, internal and territorial waters and national airspace – it seems well settled that any non-consensual intrusion qualifies as a breach of the principle of territorial sovereignty. Non-consensual intrusions of this type can be characterised as a 'wrong to personality'; to wit, it is the *mere trespass* into territory that constitutes an internationally wrongful act. It on this basis that, in the *Nicaragua* case, the ICJ concluded that the US's overflights of Nicaraguan airspace constituted a breach of the principle of territorial sovereignty. Similarly, the International Group of Experts (IGE) who compiled the Tallinn Manual 2.0 agreed that close access cyber espionage breaches the principle of territorial sovereignty due to the fact that it involves a State agent stepping into the territory of another State without consent.[91]

How the principle of territorial sovereignty applies to cyberspace and in particular to remotely conducted cyber operations has divided States and international lawyers. This issue was considered by the IGE and, under Rule 4, the Tallinn Manual 2.0 explains that '[a] State must not conduct cyber operations that violate the sovereignty of another State'. However, the IGE could reach no consensus on 'when' that occurs. Some experts considered that any cyber intrusion, however minimal in its effects, may be sufficient to breach the principle of territorial sovereignty; yet, the majority considered that cyber operations breach the principle only when they reach a certain threshold, i.e., when they produce physical damage or injury, loss of functionality in cyber infrastructure, or usurp or interfere with governmental functions of the target State.

In relation to espionage, this ongoing debate has several implications, notably for remote access cyber espionage operations that are not accompanied by any kind of physical damage or injury or loss of functionality. Is the mere hacking into a State's computer system or network that stores confidential information enough to breach the rule of territorial sovereignty?

The opinion of States appears to be coalescing around two main trends.[92] On the one hand, the first approach remains true – and gives place of pride to – one of the prime characteristics of the principle of territorial sovereignty as a cause of action: the *wrong to personality*. By this view, any cross-border penetration of computer systems or networks supported by cyber infrastructure physically located within a State's territory may constitute a breach of the rule, regardless of whether it gives rise to any form of damage and irrespective of whether the cyber infrastructure interfered with is publicly or privately owned.[93] The second approach, on the other hand, echoes that of the Tallinn Manual 2.0 in considering that a certain *threshold* is required to breach the principle of territorial sovereignty in cyberspace. We can call this the *de minimis* approach.

---

[91] Tallinn Manual 2.0 (n 24) 19, 171.

[92] For overviews of States' positions on these issues see Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, Chatham House (2019) https://www.chathamhouse.org/publication/application-international-law-state-cyberattacks-sovereignty-and-non-intervention accessed 9 December 2020 and Przemysław Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views* (2020) https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views accessed 9 December 2020.

[93] For academic support for this view see Russell Buchan, *Cyber Espionage and International Law* (Hart 2018) 51–5 and François Delerue, *Cyber Operations and International Law* (CUP 2020) 258–9.

Different States support different approaches. For instance, the French and Iranian positions come closest to the wrong to personality approach. According to France, '[a]ny unauthorised penetration by a State of French systems or any production of effects on French territory via a digital vector may constitute, *at the least*, a breach of sovereignty'.[94] By this view, any penetration of 'French systems'[95] may constitute at the least a breach of sovereignty, independently of the effects produced by this penetration.[96] France further indicates that '[t]he decision whether or not to respond to such operations is a political one, taken in light of the nature and characteristics of the intrusion'.[97] Thus, while France appears to recognise that several factors must be brought to bear on the legal analysis, it accepts that an unauthorised penetration *simpliciter*, which merely compromises the confidentiality, integrity or availability of information, is enough to breach the rule.

Similarly, Iran has expressed the view that territorial sovereignty extends 'to all the elements' of cyberspace and that 'any utilization involving unlawful intrusion to the (public or private) cyber structures' under the control of another State may constitute a breach of the target State's sovereignty, thereby adopting a wrong to personality approach.[98]

The reaction of Latin-American States[99] to the 2013 Edward Snowden revelations also supports the argument that the principle of territorial sovereignty prohibits non-consensual cyber intrusions into computer networks and systems supported by cyber infrastructure located on State territory. As these reactions were in response to disclosures concerning the US's involvement in cyber espionage operations, they are particularly important in the context of the present discussion. For example, the Foreign Minister of Venezuela submitted a *Note Verbale* to the UN Secretary-General '[c]ondemning the acts of espionage carried out by intelligence agencies of the United States of America … [which] constitute unacceptable behaviour that violates our sovereignty'.[100] Separately, the Foreign Minister of Venezuela

---

[94] *Droit International Appliqué aux Opérations dans le Cyberespace* (n 77) 6. Interestingly, the original French version of the document uses the expression 'a minima' which is translated to the phrase 'at the least' in the English version.

[95] Ibid., 6. French systems include 'equipment and infrastructure located on national territory; connected objects, logical components and content operated or processed via electronic communication networks which cover the national territory or from an IP address attributed to France; domains belonging to national registers'.

[96] This interpretation of the French statement is further supported by the use of the disjunctive 'or' in the sentence, as well as the definition provided by it for the term 'cyberattack', which it defines broadly as including cyber operations affecting the availability, integrity, or confidentiality of information. Elsewhere, the document likewise explains that '[i]n international law, a cyberoperation is not unlawful per se but can become so *where it* or its effects entail violations of international law' (our emphasis). For a different take on the French statement, see Michael N Schmitt, 'The Defense Department's Measured Take on International Law in Cyberspace '(11 May 2020) *Just Security*, https://www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/ accessed 9 December 2020.

[97] Ibid., 7.

[98] See Statement of the General Staff of Iranian Armed Forces, *General Staff of Iranian Armed Forces Warns of Though Reaction to Any Cyber Threat* (July 2020) https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat accessed 9 December 2020.

[99] Including Argentina, Bolivia, Brazil, Uruguay and Venezuela.

[100] *Note Verbale* dated 22 July 2013 from the Permanent Mission of the Bolivarian Republic of Venezuela to the United Nations addressed to the Secretary-General, UN Doc. A/67/946 (29 July 2013) 2.

explained before the Security Council that 'we reject the actions of global espionage carried out by the Government of the United States, which undermine the sovereignty of States'. He also called on the UN to 'punish and condemn this violation of international law'.[101] Brazil likewise expressed the view that cyber espionage violates international law.[102] Seemingly, the basis for these condemnations is the principle of territorial sovereignty.

China's reaction to the Snowden revelations echoes that of Latin-American States. In a speech delivered at the National Congress of Brazil in 2014, President Xi Jinping expressed that '[n]o matter how developed a country's Internet technology is, it just cannot violate the information sovereignty of other countries'.[103] On another occasion, he declared that the US's cyber espionage operations had 'flagrantly breached International laws, seriously infringed upon the human rights and put global cyber security under threat'.[104]

By contrast, the Netherlands appears to support the *de minimis* standard,[105] although it recognises that 'the precise boundaries of what is and is not permissible have yet to fully crystallise'.[106] It explains that the lack of consensus among States is due to the firmly territorial and physical connotations of the traditional concept of sovereignty. In relation to data stored using a cloud-based system, it notes that, because data is often moved from one location to another, it is 'by no means always possible to establish whether a cyber operation involves a cross-border component and thus violates a country's sovereignty'.[107] The US,[108] New Zealand[109] and the Czech Republic[110] also appear to have endorsed the *de minimis* standard. It is worthwhile adding that, regarding the Netherlands, its *de minimis* understanding appears to

---

[101] Security Council, 7015th meeting, S/PV.7015 (6 August 2013) 8.

[102] See 'Brazilian President: US surveillance a "breach of international law"', *The Guardian* (24 September 2013) www.theguardian.com/world/2013/sep/24/brazil-president-un-speechnsa-surveillance accessed 9 December 2020.

[103] Xi Jinping, 'Carry Forward Traditional Friendship and Jointly Open up New Chapter of Cooperation' (1 September 2014).

[104] Quoted in 'China demands halt to 'unscrupulous' US cyber-spying', *The Guardian* (27 May 2014) https://www.theguardian.com/world/2014/may/27/china-demands-halt-unscrupulous-us-cyber-spying (last accessed 14 August 2021).

[105] Netherlands, Appendix: International Law in Cyberspace (n 88) 3, 'In general the government endorses Rule 4, proposed by the drafters of the Tallinn Manual 2.0, on establishing the boundaries of sovereignty in cyberspace.

[106] Ibid., 2.

[107] Ibid.

[108] Though the US's position remains one of studied ambiguity. See Hon. Paul C. Ney Jr., 'DOD General Counsel Remarks at U.S. Cyber Command Legal Conference' (2 March 2020), 'it does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law' https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/ accessed 9 December 2020. See also Harold Hongju Koh, Legal Advisor, US Department of State, *Remarks at USCYBERCOM Inter-Agency Legal Conference: International Law in Cyberspace* (18 September 2012) https://2009-2017.state.gov/s/l/releases/remarks/197924.htm accessed 9 December 2020; Brian J Egan, Legal Adviser, US Department of State, *Remarks on International Law and Cyberspace* (10 November 2016) https://2009-2017.state.gov/s/l/releases/remarks/264303.htm accessed 9 December 2020. For further discussion of the US's position see Russell Buchan, 'When More is Less: The US Department of Defense's Statement on Cyberspace' (30 March 2020) EJIL: *Talk!*, https://www.ejiltalk.org/when-more-is-less-the-department-of-defenses-statement-on-cyberspace/ accessed 9 December 2020.

[109] New Zealand (n 86) para 14.

[110] Kadlčák (n 87).

be circumscribed to *remote access* cyber intrusions. In cases of close access cyber espionage targeting international organisations on its territory, such as that of Russia's GRU operations targeting the OPCW offices in The Hague, the Netherlands has firmly condemned these acts.[111]

Both approaches have their merits. On the one hand, the *de minimis* approach allows for flexibility and the emergence of a cyber-specific understanding of the principle of territorial sovereignty. Such proviso can also be extrapolated from State practice predating cyberspace, which suggests that this position possess a certain pedigree. By way of example, there is a consensus that remote sensing activities carried out from outer space by satellites are permissible because the satellites do not physically intrude upon the sensed-States' sovereignty and remain at all times in outer space.[112] Be that as it may, the fact remains that remote sensing activities are not completely innocuous; they still involve a *minimal* element of intrusion with the sending of an electromagnetic pulse from the satellite to the sensed-States' territory and its reflectance/scattering measured.[113] From this perspective, it could be argued that remote sensing activities breach the sensed-States' sovereignty. Yet, no State has ever protested this technical aspect of remote sensing activities. As one of the present authors contends elsewhere,[114] this example suggests that a *de minimis* standard to the principle of territorial sovereignty may be teased out from State practice and similarly applied to cyberspace.

This makes intuitive sense. The law, after all, does not concern itself with trifles, and it is natural that the principle of territorial sovereignty should incorporate *some* internal limitation so as not to extend its aegis to innocuous and commonplace cyber operations, which ought to be treated commensurately by States. This is especially true where the encroachment on another State's sovereignty is technical and derives from the structure of cyberspace itself.

On the other hand, there are equally powerful reasons for favouring the 'wrong to personality' understanding of sovereignty in cyberspace. For one, there seems no be no principled reason for regarding the rule of territorial sovereignty as providing a State's sovereign *cyber* infrastructure with less protection from intrusion than a State's sovereign *physical* territory.[115] And, as we have seen, the breach of this rule does not require the infliction of physical damage or harm. In this way, the rule provides, especially for those States that do not necessarily

---

[111] 'Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW' https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw, 'The Netherlands shares the concerns of other international partners regarding the damaging and undermining the GRU's actions. It supports the conclusion, presented today by the UK, that GRU cyber operations such as this one undermine the international rule of law' accessed 9 December 2020.

[112] See generally Bin Cheng, 'The Legal Regime of Airspace and Outer Space: The Boundary Problem Functionalism versus Spatialism: The Major Premises' (1982) 19 *Annals of the Chinese Society of International Law* 1. See also Thomas Gangale, *How High is the Sky? The Definition and Delimitation of Outer Space and Territorial Airspace in International Law* (Brill 2018).

[113] Generally speaking, active sensors generate radiation and measure the return signal after interaction with the object of interest, whereas passive sensors rely on object generated/reflected radiation. For a different perspective on this point see Craig Forcese, 'Pragmatism and Principle: Intelligence Agencies and International Law' (2016) 102 *Virginia Law Review Online* 67, 80, challenging the analogy between remote access cyber espionage and remote sensing activities: 'This is not like remote sensing involving passive sensors located outside the territory of the state. Instead, this involves the transmission of electrical impulses in a manner that changes (and does not simply observe) the status quo in a foreign state'.

[114] Iñaki Navarrete, 'L'Espionnage en Temps de Paix en Droit International Public' (2015) 53 *Canadian Yearbook of International Law* 1, 24.

[115] Buchan (n 93) 54.

possess the cyber wherewithal of other States, a desirable guarantee against intrusions into their sovereign affairs. Finally, to integrate a *de minimis* threshold into the principle of territorial sovereignty complexifies its application and raises difficult questions about which types of activities are sufficiently serious to fall within its scope.

Ultimately, the question of what types of cyber operations breach the principle of territorial sovereignty can only be determined by developments in State practice. Because there is, as of yet, no cut and dried answer to the question of how the rule of territorial sovereignty operates in cyberspace, there is not cut and dried answer to the question of whether remote access cyber espionage operations breach the rule. This being said, State practice on cyber espionage is likely to remain rather limited given the policy of silence that surrounds espionage, combined with the fact that cyberspace is a domain that lends itself to anonymous activities.

5. ECONOMIC CYBER ESPIONAGE AND THE WORLD TRADE ORGANIZATION

Recognising the threat that economic espionage represents to national security, a number of States (such as Australia, Canada, the US and the UK) have signed bilateral agreements declaring that they will not engage in economic cyber espionage.[116] In 2015, the G20 leaders issued a joint communiqué affirming that 'no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors'.[117] Crucially, these initiatives do not impose binding commitments upon the issuing States, although one commentator has noted that these soft law agreements may eventually snowball into a hard rule of customary law that specifically prohibits economic cyber espionage.[118]

In terms of positive international law applicable to economic cyber espionage, the law of the World Trade Organization (WTO) comes into focus. The WTO is an international organisation overseeing numerous treaties that are designed to protect a variety of trade-related rights.

The Paris Convention for the Protection of Industrial Property 1967 (Paris Convention) is the WTO treaty that is most relevant when it comes to regulating economic cyber espionage. Article 10*bis*(1) of the Paris Convention requires States parties to 'assure to nationals' of other States parties 'effective protection against unfair competition'. As understood by the Convention, nationals include natural[119] as well as legal persons,[120] that is, individuals granted

---

[116] Ellen Nakashima and Steven Mufson, 'The U.S. and China Agree Not to Conduct Economic Espionage in Cyberspace', *Washington Post* (25 September 2015) https://www.washingtonpost.com/world/national-security/the-us-and-china-agree-not-to-conduct-economic-espionage-in-cyberspace/2015/09/25/1c03f4b8-63a2-11e5-8e9e-dce8a2a2a679_story.html accessed 9 December 2020.

[117] G20 Leaders' Communiqué, 15–16 November 2015, https://www.consilium.europa.eu/media/23729/g20-antalya-leaders-summit-communique.pdf accessed 9 December 2020.

[118] Martin Libicki, 'The Coming of Cyber Espionage Norms' in Henry Rõigas, Raik Jakschis, Lauri Lindström and Tomáš Minárik (eds), *Defending the Core* (CCDCOE 2017).

[119] Art 2.1 Paris Convention.

[120] Art 2.1 Paris Convention does not expressly state that legal persons constitute nationals. Yet, that Art 2.1 includes legal persons (companies) is indicated by Art 1.3 of the Agreement on Trade-Related Aspects of Intellectual Property Rights 1994, which explains that 'nationals of other Members shall be understood as those natural or legal persons that would meet the criteria for eligibility for protection provided for in the Paris Convention (1967)'.

nationality by the domestic law of States parties and companies incorporated under that law. Moreover, nationals of States not party to the convention benefit from the protection it affords when individuals are 'domiciled' within the territory of a State party and, significantly with regard to economic cyber espionage, when companies operate 'real and effective industrial or commercial establishments' within such territory.[121]

States usually conduct economic cyber espionage against companies located in *foreign jurisdictions*. This raises the question of whether Article 10*bis*(1) of the Paris Convention imposes an obligation upon States parties to protect nationals from unfair competition when they are located outside their territory. Commentators such as Strawbridge[122] and Fidler[123] have argued that WTO law (including the Paris Convention) does not impose obligations upon States parties when acting extraterritorially and, for this reason, they conclude that the WTO offers little protection against remote access economic cyber espionage.

However, whether a treaty obligation applies extraterritorially depends on the construction of that obligation as well as the object and purpose of the treaty.[124] If we look at the language of Article 10*bis*(1), there is no evidence to suggest that States parties must only protect Paris Convention nationals from unfair competition when they are located within their own territory. In fact, the language of Article 10*bis*(1) is broad and appears to impose a general obligation upon States parties to protect Paris Convention nationals from unfair competition. Additionally, Article 10*bis*(2) explains that '[a]ny act of competition contrary to honest practices' constitutes unfair competition.

Of course, the extraterritoriality of Article 10*bis*(1) does not mean that States parties must actively protect Paris Convention nationals from all acts of unfair competition while they are within foreign territory. Such a construction would impose arduous and unreasonable burdens upon States parties. But what it does mean is that – as international courts have decided in the context of the extraterritoriality of human rights treaties[125] – States parties are prohibited from exercising their *authority and control* over Paris Convention nationals located in foreign territory in a manner that amounts to unfair competition.

The immediate question is whether economic cyber espionage amounts to unfair competition. As we have seen, Article 10*bis*(2) defines unfair competition as '[a]ny act of competition contrary to honest practices in industrial or commercial matters'. Article 10*bis*(3) provides a list of acts that qualify as unfair competition, and it is apparent that economic espionage is not identified as an example of unfair competition. However, Article 10*bis*(3) identifies exam-

---

[121] Art 3 Paris Convention.

[122] 'WTO rules generally operate on a territorial basis; that is, Members are only obligated to act in accordance with WTO rules with respect to goods, services, and investments of foreign nationals that enter or take place within their territory'; Jamie Strawbridge, 'The Big Bluff: Obama, Cyber Economic Espionage, and the Threat of WTO Litigation'(2016) 47 *Georgetown Journal of International Law* 833, 852–3.

[123] 'WTO rules create obligations for WTO members to fulfill within their territories and do not generally impose duties that apply outside those limits'; David P Fidler, 'Economic Cyber Espionage and International Law: Controversies Involving Acquisition of Trade Secrets through Cyber Technologies' (29 March 2013) *ASIL Insights*, https://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving accessed 9 December 2020.

[124] Marko Milanovic, 'The Spatial Dimension: Treaties and Territory' in Christian J Tams, Antonios Tzanakopoulos and Andreas Zimmermann, with Athene W Richford (eds), *Research Handbook on the Law of Treaties* (Edward Elgar 2016).

[125] See, e.g., *Al-Skeini v United Kingdom*, Judgment, App No 55721/07, ECtHR, 7 July 2011.

ples of unfair competition that are 'in particular … prohibited', which indicates that the list is not intended to be exhaustive. The question, then, becomes whether cyber espionage qualifies as 'unfair competition'.

To establish an act of unfair competition, two elements must be present. First, there must be an act of *competition* and, second, it must be *unfair*. In relation to the first element, it could be argued that economic cyber espionage does not qualify as an act of competition because the perpetrating State is not a competitor of the victim company.[126] Yet, in recent years the definition of an act of competition has moved away from an assessment of the structural relationship between the offender and victim and instead focuses upon the impact of the activity on the market. Thus, it is accepted that conduct qualifies as an act of competition when it inhibits the 'competitive opportunities of nationals of other [Paris Convention] Members'.[127] In light of this, it is clear that the theft of a company's trade secrets impairs its competitive opportunities and also has a wider chilling effect on the market.

With regard to the second requirement that the act of competition must be unfair, this demands an analysis of whether the act of competition amounts to a dishonest commercial practice within the meaning of Article 10*bis*(2) of the Paris Convention. The answer to this question is straightforward given that the theft of a company's trade secrets obviously constitutes a dishonest commercial practice.

The key advantage of framing an act of economic cyber espionage as a violation of the Paris Convention is that a WTO member State could bring proceedings against another member before the WTO's Dispute Settlement Body (DSB). All States parties of the WTO are members of the DSB. The DSB also has compulsory jurisdiction over disputes in the sense that, when a member lodges a complaint with the DSB and the DSB's attempts to resolve the dispute through negotiation fail, a Panel must be established unless the DSB decides by consensus to reject it.[128]

As any court or tribunal, a Panel can determine that a member has engaged in conduct that violates WTO law. Moreover, where the unlawful conduct is ongoing (as would be the case where a State is engaged in a systematic campaign of economic cyber espionage), a Panel can request that the offending member remedy the violation and bring its behaviour into conformity with WTO law.[129] If the offending member fails to comply, the DSB can authorise the victim member to engage in measures that would otherwise violate WTO where the objective is to push the offending member into law-compliance.[130]

---

[126] Commission Decision of 23 December 1988 rejecting the complaint lodged by Smith Kline and French Laboratories Limited Against Jordan under Council Regulation (EEC) No 2641/84 Decision 89/74/EEC, Official Journal L 030, 01/02/1989, para 10.

[127] Christian Riffel, *Protection Against Unfair Competition in the WTO TRIPS Agreement: The Scope and Prospects of Article 10bis of the Paris Convention for the Protection of Industrial Property* (Brill 2016) 76.

[128] Art 6.1 of the Understanding on Rules and Procedures Governing the Settlement of Disputes.

[129] Ibid., art 19.1.

[130] Ibid., art 22.2.

6. CONCLUSION

Having presented political and economic cyber espionage as a potential threat to the maintenance of international peace and security, the core objective of this chapter has been to examine whether and to what extent international law regulates this conduct. For many, espionage is a 'dirty word'[131] that is not discussed in 'polite company'.[132] This reticence partly explains why States have failed to develop an 'international law of espionage' in the same way that they have created the law of the sea, the law of war, international human rights law, international environmental law, etc.[133] But the absence of *lex specialis* on espionage does not mean that this conduct is immune from the regulatory purview of international law. On the contrary, and providing one is prepared to look carefully, there is international law *on* espionage, and which can apply to cyber-enabled espionage. In this way, cyber espionage must be studied by examining its interface with disparate areas of international law such as general principles and specialised regimes.

In terms of general principles of international law, this chapter examined whether political and economic cyber espionage breaches the principle of territorial sovereignty. In the first instance, this chapter demonstrated that the principle of territorial sovereignty is a stand-alone rule of international law.

There can be little doubt that close access cyber espionage operations breach the principle of territorial sovereignty and they do so on the basis that they involve non-consensual intrusions into the physical territory of other States. Whether remote access cyber espionage operations breach the rule of territorial sovereignty remains unsettled. In short, different views have emerged. One argument is that any non-consensual intrusion into the territory of another State – including the cyber infrastructure located on that territory – constitutes a breach of the principle of territorial sovereignty. Another view is that a *de minimis* threshold is built into the principle of territorial sovereignty or should exist when this principle operates in cyberspace, meaning that a breach occurs only where the impugned conduct gives rise to sufficiently serious adverse effects for the target State. For proponents of this view, acts of cyber espionage are not sufficiently serious to trigger a violation of the rule of territorial sovereignty. Which approach prevails is a critically important question for international law and, ultimately, it can only be resolved through State practice.[134]

With regard to specialised regimes of international law, this chapter analysed whether WTO law applies to economic cyber espionage. In particular, this chapter demonstrates that economic cyber espionage constitutes a dishonest commercial practice and therefore can amount to an act of unfair competition contrary to Article 10*bis*(1) of the Paris Convention. Importantly, WTO members can prosecute acts of economic cyber espionage through the WTO's DSB and, where this unlawful conduct is ongoing, the DSB can authorise victim

---

[131] International Peace Academy, Peacekeeper's Handbook (1984) 39, 59–62, 120–1.

[132] 'There are certain matters that international lawyers do not like discussing in polite company. Close to the top of any list is likely to be peacetime espionage'; Duncan French, 'Book Review: *Cyber Espionage and International Law* by Russell Buchan' (2019) 32 *Leiden Journal of International Law* 883, 883.

[133] Although Lubin argues that *lex specialis* on intelligence collection has emerged; Asaf Lubin, 'The Liberty to Spy' (2020) 61 *Harvard International Law Journal* 185.

[134] On the development of cyber norms see Lehto (Ch 2 of this Handbook).

members to engage in trade retaliation to the extent necessary to induce offending members into law compliance.

Disclaimer

The arguments advanced in this chapter are the authors alone and do not necessarily reflect the views of the institutions to which they belong.

12. International legal dimensions of cybercrime

Philipp Kastner and Frédéric Mégret

Hacked computers, virus attacks, interference with elections, massive spam, online fraud, harassment in cyberspace or 'cyberstalking' – networked technology has given rise to a new, yet apparently ubiquitous phenomenon: cybercrimes. These relatively new forms of crime, which also create large numbers of new victims and forms of victimization,[1] seem to be difficult to tackle through traditional criminal law responses. Does that mean that States are really losing the fight against cybercrime, as a British Parliamentary Committee warned in 2013?[2] Or does the cyber-realm merely pose in new ways age-old questions of law enforcement and criminal justice?

The internet age has certainly transformed social relations and the economy in ways that suggest that criminal behaviour will follow suit. Cyberspace has opened up a whole range of new opportunities for criminal activity that challenge traditional approaches based on jurisdiction and law enforcement by the nation-State.[3] Communication has become fast and easy. It often transits through multiple jurisdictions, sometimes in an automated manner. Conventional crimes, like theft and fraud, are increasingly facilitated by technology and may now take wholly different forms that hardly existed even a decade ago. In many instances, the offenders and victims of a harmful conduct are not located in the same jurisdiction.

Keeping up with these evolutions has been a challenge for a criminal justice framework that remains, by and large, jurisdiction and territory-bound. Notwithstanding, it is because of this typically deterritorialized nature of cybercriminal activities that legal responses themselves have increasingly taken an inter- or transnational dimension. This has not been a hurdle-free process: with States typically wanting to hold on to their sovereignty, of which prescriptive and enforcement jurisdiction over criminal matters is an emblematic element, adoption and harmonization of relevant legislation as well as cooperation between States to combat cybercrime have emerged as major issues.

In this chapter, we will focus on cybercriminal activities that cannot easily be regulated by States via already existing means, either because new criminal elements are involved or because the scale and the transnational element in a particular illicit activity necessitate international cooperation. While many crimes committed by means of a computer are not essentially new crimes and can be subsumed under extant definitions and be dealt with by domestic legal systems, some criminal activities require specific legal responses at the international level. This chapter will give an overview of these crimes, examine initiatives that have been undertaken to fight them, and discuss particular challenges, notably with respect to jurisdiction.

---

[1] Elena Martellozzo and Emma A Jane (eds), *Cybercrime and its Victims* (Routledge 2017).

[2] 'UK "losing" fight against internet crime, warn MPs', *BBC News* (30 July 2013) http://www.bbc.co.uk/news/uk-politics-23495121.

[3] See Kohl (Ch 4 of this Handbook).

1. THE PHENOMENON OF CYBERCRIME

Cybercrime, which is sometimes also called e-crime, computer crime, net crime, internet crime or network crime,[4] has been defined and categorized in various ways. In a broad sense, a cybercrime consists of 'a crime committed against a computer or by means of a computer',[5] in other words in any criminal activity involving computer technology. What is interesting about the definition therefore is that it focuses on the instrument or possibly the context or environment rather than the specific social harm caused. Cyberspace can thus be a conduit for crime, although it is also a realm that needs to be protected from it.

Cybercrimes may result in harm to property or in harm to persons.[6] They have developed from the use of computers to prepare crimes, to offences mediated almost entirely by technology such as spamming.[7] Computer technology has become central to the commission of various crimes which only exist, at least in their specific form, as a result of the existence of computer systems. Online fraud, forgery, and 'phishing' fall into this category. Computers and computer systems may also be the target or 'victim' of cybercriminal activities. These so-called computer integrity crimes include illegal access to computer data or systems, commonly referred to as 'hacking' or 'cracking'; the dissemination of malicious software, such as viruses and worms; and denial of service attacks that may even represent a method of modern terrorism.[8] Finally, cybercriminal activity may relate to a specific content, with the dissemination of child pornography and hate speech figuring most prominently in this category. The internet may also more generally serve as a site of distribution of illicit products, such as counterfeits.[9]

Due to the increasing digitalization of social relations, it may become necessary to add another category: 'crimes' committed in virtual worlds such as *Second Life* or in so-called 'massively multi-player online role-playing games' (MMORPGs). Theft of virtual property, virtual rape and sexual harassment as well as virtual paedophilia could and should arguably be regulated by the operator of the respective virtual 'world'. However, such conduct may also have significant consequences in the real world and may hence require a response from ordinary legislators as well, or in addition to cyber-specific responses.

For instance, virtual property is widely traded online and paid for with real money. This means that stolen virtual property also has value in the real world. The person behind a sexually harassed avatar may suffer emotional harm and be traumatized in the same way as a victim of conventional harassment. It is still unclear to which extent the 'real' world – including law-enforcement authorities – should be concerned with such 'virtual' crimes. It has been argued that virtual crimes are always 'grounded in physical reality' and that, without harm in

---

[4] For additional terms, see Jonathan Clough, *Principles of Cybercrime* (CUP 2010) 9.

[5] Bernadette H Schell and Clemens Martin, *Cybercrime: A Reference Handbook* (ABC-CLIO 2004) 29.

[6] For this categorization, see ibid., 30.

[7] For this differentiation, see David S Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity 2007) 44–8.

[8] For more information on cyber terrorism and cyber warfare, see Saul and Heath (Ch 10 of this Handbook) and also Part IV of this Handbook.

[9] Michael M DuBose, 'Criminal Enforcement of Intellectual Property Laws in the Twenty-First Century Symposium: How the Show Goes On: Law and Theater in the Twenty-First Century' (2005) 29 *Columbia Journal of Law & the Arts* 481.

the real world, there is no cybercrime.[10] Yet what counts as 'real' especially in the psychological or economic realms may always have been quite elusive. Moreover, it is not as if connections do not exist between the two: some virtual behaviour, even without causing direct harm in the real world, can arguably contribute to downplaying and normalizing an activity that is criminalized in the physical world, an obvious example being paedophilia.[11] Some national criminal systems have responded to such phenomena.[12]

In addition to its virtuality, cybercrime has often taken on strongly transnational connotations. It is of course perfectly possible for cybercrime to occur entirely within the jurisdiction of a single State. More often than not, however, precisely what cybercrime makes possible is moving seamlessly between different jurisdictions – exploiting, in fact, existing gaps between such jurisdictions.[13] This is not entirely new: criminal organizations and networks for example have long expanded and collaborated across borders. The novelty of the cheapening and democratizing of digital communication technologies, however, is that they have drastically lowered the costs of operating cross-border for new actors, even as they have provided older ones with new modalities of doing so.[14] Cybercrime, more than any other form of criminality before it, may be inherently global.[15]

2. THE INTERNATIONAL SUBSTANTIVE LAW OF CYBERCRIME

Several initiatives have been launched at the international level to respond to cybercrime, notably by harmonizing existing legislation, defining 'new' crimes and by trying to enhance transnational cooperation. These are a fairly conventional way of dealing with transnational criminal problems that has long been experimented with in other contexts and the conventions do not necessarily break any new ground aside from their subject matter.

The most important of these initiatives is the Convention on Cybercrime of the Council of Europe (Budapest Convention) that entered into force in 2004.[16] The first multilateral and most relevant treaty in the field, and unlike other instruments of the Council of Europe (CoE) open to all States, this instrument could, at least theoretically, become applicable universally.

---

[10] Susan W Brenner, 'Fantasy Crime' (2008) 11 *Vanderbilt J of Technology and Entertainment L* 1, 26.

[11] A good example is virtual ageplay, where all players are adults but engage, via their avatars, in sexual behaviour between children and adults. For an overview over the main arguments, see ibid., 42–3. For the reasoning of the Supreme Court of Canada regarding child pornography fuelling fantasies that incite offenders, see *R v. Sharpe* 2001 SCC 2.

[12] The arrest of a Dutch teenager in 2007 for stealing virtual furniture on *Habbo* is only one example. See '"Virtual Theft" Leads to Arrest', *BBC News* (14 November 2007) http://news.bbc.co.uk/2/hi/7094764.stm. In some States, such as in South Korea, where virtual worlds are particularly popular, law enforcement authorities have created specialized divisions to address such 'crimes'.

[13] Ellen S Podgor, 'Cybercrime: National, Transnational, or International Symposium' (2004) 50 *Wayne Law Review* 97.

[14] James R Richards, *Transnational Criminal Organizations, Cybercrime, and Money Laundering: A Handbook for Law Enforcement Officers, Auditors, and Financial Investigators* (CRC Press 1998).

[15] Peter Grabosky, 'The Global Dimension of Cybercrime' (2004) 6 *Global Crime* 146.

[16] Convention on Cybercrime (Council of Europe), CETS No. 185, 23 November 2001 (entered into force: 1 July 2004).

While, initially, mostly Western States, including such non-CoE members as the United States, Australia and Japan, joined the Convention, a significant number of States from all regions, including Argentina, Morocco, the Philippines, Senegal and Tonga, have acceded to the Convention in recent years.[17] It should also be noted that in addition to being the most widely ratified legally binding instrument, the Convention has provided guidance for or, at least inspired, the drafting of national cybercrime legislation in about 150 States.[18]

Other instruments dealing with cybercrime have been developed in several regions. These include the 2010 League of Arab States Convention on Combating Information Technology Offences; the 2001 Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information; the 2010 Shanghai Cooperation Organization Agreement in the Field of International Information Security; and the 2014 African Union Convention on Cyber Security and Personal Data Protection (AU Convention). While these instruments are inspired by the Budapest Convention and adopt similar concepts and approaches,[19] a few important differences exist. The AU Convention, for instance, does not envisage the establishment of mechanisms for cooperation in cybercriminal matters but focuses more generally on cybersecurity; combating cybercrime is therefore only one approach, along with the organization of electronic transactions, personal data protection and the promotion of cybersecurity.[20] In Europe, another important yet purely regional instrument is the Framework Decision adopted by the Council of the European Union in 2005.[21] With respect to substantive law, this Framework Decision on attacks against information systems resembles the Budapest Convention in many respects;[22] the Framework Decision is, however, more specific with respect to the procedural law, in particular when it comes to jurisdiction.[23] Finally, efforts have also been made to adopt a convention within the United Nations frameworks. Russia, for instance, proposed a 'Draft United Nations Conventions on Cooperation in Combating Cybercrime' in 2017.[24]

---

[17] As of November 2019, there were 64 States parties to the Budapest Convention. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

[18] Council of Europe, Cybercrime Programme Office, *The global state of cybercrime legislation 2013 – 2019: A cursory overview* (30 June 2019) https://rm.coe.int/the-global-state-of-cybercrime-legislation-2013-2019-a-cursory-overvie/168095da1f.

[19] For a thorough comparison of these instruments, see UN Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (February 2013) http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf 63–72 and Annex Three. For a study of the Southern African Development Community's Model Law on Computer Crime and Crime, itself modelled on the Budapest Convention and adopted in 2012, and of examples of domestic legislation in the region, see Lewis C Bande, 'Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities' (2018) 12 *International Journal of Cybercriminology* 9.

[20] African Union Convention on Cyber Security and Personal Data Protection, 27 June 2014 (not yet entered into force).

[21] Council of the European Union, Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[22] For a more detailed comparison between the two instruments, see Paul De Hert, Gloria Gonzáles Fuster and Bert-Jaap Koops, 'Fighting Cybercrime in the two Europes' (2006) 77 *Revue internationale de droit pénal* 503.

[23] Council Framework Decision 2005/222/JHA (n 21) section 4.

[24] Letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary General, 16 October 2017, UN Doc A/C.3/72/12. However,

A significant challenge in the global fight against cybercrime lies in the fact that similar activities may be considered a crime in some countries, such as a massive spam attack against a specific person or company, but simply an unwanted behaviour in others akin to, in the case of spam, conventional unsolicited publicity by a company. 'Hacking' and 'cracking' are more likely to be considered harmful activities, to be outlawed and penalized. But how should we deal with hackers who do not necessarily act with criminal intent but enter systems for fun or with so-called hacker activists or 'hacktivists' who seek, for instance, to circumvent excessive restrictions and online surveillance of repressive governments?

Even if there exists a general consensus among States regarding which acts – broadly speaking – should be criminalized,[25] opinions and approaches diverge when it comes to the details. There may, for instance, exist a consensus on the criminalization of a certain conduct related to the content of webpages in some jurisdictions; in others, such criminalization would be seen as unduly limiting the freedom of expression. Child pornography and hate speech are again good examples, which reflect quite dissonant national approaches.[26] Issues relating to intellectual property have also proved divisive, particularly as between developed and developing States, and explain why a country like Brazil declined to sign the Budapest Convention.

The problem is that if not restricted and prohibited globally, in other words without exception, the relevant content may always resurface – legally – on the internet and be accessible from anywhere in the world. One 'hole' in the system is sufficient to make, by default, any content available on a global scale. Similar problems arise in the context of copyright. What may be promoted as 'open access' or 'freedom of the internet' in one place may represent grave infringements of intellectual property rights elsewhere. In short, what used to be local problems that could easily be dealt with domestically now require not only concerted efforts but also far-reaching compromises between legislations. With respect to content-related cybercrimes, however, the territorial restriction of websites may be an alternative to the harmonization of substantive legal rules.

The Budapest Convention is a convenient starting point to discuss current efforts to criminalize cybercrimes because of its fairly wide ratification and its helpful approach to the classification of offences.[27] The Convention itself does not criminalize certain acts but requires States parties to adopt 'legislative and other measures' to ensure that the offences

---

it seems that many States do not consider it necessary to adopt another treaty, with existing instruments, above all the Budapest Convention, already providing useful guidance and facilitating international cooperation. See, e.g., UNODC, *Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 March 2019* (12 April 2019), UN Doc UNODC/CCPCJ/EG.4/2019/2, para II.A.b. For a poignant critique of this proposed convention, in which dozens of human rights organizations affirm that it 'could undermine the use of the internet to exercise human rights and facilitate social and economic development', see 'Open letter to UN General Assembly: Proposed international convention on cybercrime poses a threat to human rights online' (November 2019) https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human.

[25] For the summary findings of a survey conducted by the UN Office on Drugs and Crime, to which 56 States responded, see UNODC/CCPCJ/EG.4/2013/2, paras 13–15.

[26] For the recurrent problem of enforcement between different jurisdictions, in this case because of the accessibility of illegal material in France through a US-based internet provider, see *Yahoo! v. La Ligue contre le racisme et l'antisémitisme* 433 F.3d 1199 (9th Cir. 2006).

[27] On the applicability, yet limited usefulness, of customary international law and general principles of international law, see Ilias Bantekas, 'Cybercrime and its Sovereign Spaces' in Harmen van der Wilt

listed in the treaty are 'punishable by effective, proportionate and dissuasive sanctions' (art 13). With respect to substantive law, the Convention divides the activities that the States parties are required to criminalize into four categories: offences against the confidentiality, integrity and availability of computer data and systems, such as illegal access and interception; computer-related offences, namely computer-related forgery and fraud; content-related offences, the only one being related to child pornography; and offences related to the infringement of copyright and related rights. An additional protocol to the Convention that entered into force in 2006[28] pertains to another content-related offence, namely the dissemination of racist and xenophobic material on the internet.

The offences contained in the first category are offences in which a computer or computer system is targeted intentionally. 'Illegal access' refers to the 'access to the whole or any part of a computer system without right' (art 2). The enormous amount of information stored electronically includes much information that is meant to remain confidential, such as credit card numbers and medical records, defence secrets and other sensitive government information as well as information protected by intellectual property. Gaining access to such information may be valuable for various reasons and may be a precursor to other, possibly more serious offences, such as fraud and identity theft. Illegal access may consist in a simple unauthorized log in to a computer or system, for instance by an employee who has found or guessed the password of a colleague and logs in to her computer or e-mail account; illegal access may also represent more complex 'hacking' into another computer system, for instance by exploiting vulnerabilities in software programs.[29] It is worth noting that existing national approaches with respect to 'illegal access' vary considerably. There is notably no consensus with respect to requiring additional circumstances, such as the creation of dangers or damages by the intrusion.[30] There are also significant differences regarding the penalties for illegal access, with the maximum term of imprisonment being two years or more in roughly two-thirds of the countries responding to a survey of the UN Office for Drugs and Crimes, but six months in the case of around 15 per cent of the responding countries.[31]

The provision on 'illegal interception' aims to protect the privacy of electronic communication, similar to traditional tapping and recording of telephone communications.[32] 'Illegal interception' refers to the 'interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromag-

---

and Christophe Paulussen (eds), *Legal Responses to Transnational and International Crimes: Towards an Integrative Approach* (Edward Elgar 2017) 134.

[28] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (Council of Europe), CETS No. 189, 28 January 2003 (entered into force: 1 March 2006). In November 2019, the protocol had 32 ratifications/accessions.

[29] Clough (n 4) 28.

[30] See also Council of Europe, Convention on Cybercrime, Explanatory Report, para 49. The Budapest Convention only speaks of illegal access 'without right', which arguably includes those hackers who are driven by ethical considerations and, for instance, seek to promote privacy rights or to enhance security by carrying out penetration tests. For the distinction between 'ethical hackers' and 'unethical hackers' or 'crackers', see Wall (n 7) 54–56.

[31] UN Office on Drugs and Crime (n 19) 62.

[32] Convention on Cybercrime, Explanatory Report (n 30) para 51. The Explanatory Report, adopted by the Committee of Ministers of the Council of Europe, does not provide an 'authoritative interpretation of the Convention' but aims to 'facilitate the application' of its provisions. Ibid. para II.

netic emissions from a computer system carrying such computer data' (art 3). 'Data interference' refers to 'damaging, deletion, deterioration, alteration or suppression of computer data without right' (art 4). This provision covers the use of malicious software, such as viruses, worms and Trojan horses.[33] According to the second paragraph of the same article, States parties can add the requirement that the data interference 'result in serious harm', as defined by the domestic legislation.[34]

'System interference' means 'the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data' (art 5). So-called denial of service attacks, which seek to 'overwhelm' a network,[35] are covered under this provision. The attack against the credit card company MasterCard in retaliation for its decision to cease transferring donations to WikiLeaks, which paralyzed the system of MasterCard for several hours,[36] is a well-known example. The sending of unsolicited e-mail, or 'spamming', may also be subsumed under 'system interference' and must therefore be criminalized by the States parties when constituting a 'serious hindering' of the functioning of a system; the precise threshold of harm required is to be determined by national legislation.[37] The high proportion of spam – approximately 80–90 per cent of all e-mail sent[38] – reveals that spam is not simply a nuisance but a threat to the proper functioning of the cybersphere. However, not every sending of an unsolicited e-mail constitutes an offence. The Budapest Convention deals only with part of the problem, in other words with some of its volume-related aspects and none of its content-related aspects.[39] This seems to correspond to a widely shared consensus: no multilateral instrument requires States to establish the sending of spam as a criminal offence, and only few States have enacted such legislation.[40]

Finally, and as part of that first category, the Budapest Convention establishes as a separate offence the production and distribution of devices that are to be used to commit the above-listed offences against the confidentiality, integrity and availability of computer data and systems. Under article 6, States are thus required to criminalize the 'production, sale, procurement for use, import, distribution or otherwise making available of:

– a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above articles 2 through 5
– a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed' (art 6(1)a).

A few so-called computer-related offences seek to address the commission of ordinary crimes through the manipulation of computer systems or data. Computer related forgery refers to the

---

[33] For the distinction between these forms of malicious software, see Clough (n 4) 33–4.
[34] Convention on Cybercrime, Explanatory Report (n 30) para 64.
[35] For more information on these attacks, see Clough (n 4) 37–9.
[36] 'Operation Payback cripples MasterCard site in revenge for WikiLeaks ban', *BBC News* (8 December 2010) http://www.theguardian.com/media/2010/dec/08/operation-payback-mastercard-website-wikileaks.
[37] Convention on Cybercrime, Explanatory Report (n 30) para 69.
[38] For the comparison of several studies, see Clough (n 4) 234.
[39] For this distinction, see De Hert, Gonzáles Fuster and Koops (n 22) 510–12.
[40] For more information, see UN Office on Drugs and Crime (n 19) 95–6.

'input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic' (art 7), thus extending the forging of tangible documents to electronic data. The subsequent provision attempts to address the multiple opportunities of computer-related fraud, such as credit card fraud and the manipulation of electronic funds, and requires States parties to criminalize 'the causing of a loss of property to another person' by similar means as those listed in article 7, when committed with the intent to gain an economic benefit (art 8).

Other instruments include additional computer-related offences. The League of Arab States Convention, for instance, besides demanding that States parties criminalize computer-related fraud and forgery (arts 10 and 11), contains specific provisions on offences involving money-laundering, human trafficking and drug trafficking (art 16) as well as terrorism (art 15). The AU Convention follows another approach and requires States parties to set up as an aggravating circumstance the use of information technology to commit ordinary crimes, such as fraud, terrorism, and money laundering (art 30(1)(b)).

The only content-related offence dealt with in the Budapest Convention concerns child pornography and its production, offering, distribution, procurement or possession by using a computer system (art 9). This provision seeks to protect the sexual exploitation of persons under 18 years, since '[i]t is widely believed that such material and on-line practices, such as the exchange of ideas, fantasies and advice among paedophiles, play a role in supporting, encouraging or facilitating sexual offences against children'.[41]

In terms of consistency, it is worth highlighting that the Convention allows States to opt out from certain provisions regarding child pornography. The use of a computer system to procure or possess child pornography as well as virtual child pornography do not have to be criminalized; States may also lower the ordinary age limit of a 'child' from 18 years to up to 16 years (art 9(3)). What may appear as a minor detail reveals an inherent problem related to the intended harmonization of substantive law, which is aggravated by the fact that the Convention does not offer a model law.[42] States often want to retain some flexibility and enact laws corresponding to a societal consensus in the respective jurisdiction with respect to the appropriateness of punishment. The Budapest Convention attempts to recognize these traditional differences among States by including specific provisions like the one pertaining to the age limit in the context of child pornography and, more generally, by leaving the formulation of both substantive and procedural provisions to the domestic legislatures. This approach has nonetheless been criticized as a 'watered down compromise of flexible harmonization [that] offers little to motivate nations to voluntarily relinquish sovereignty in favor of international regulation'.[43] As we will see, this also potentially raises important jurisdictional issues.

Other instruments similarly seek to strengthen the protection of children against sexual exploitation by requiring States to establish as criminal offences various forms of conduct relating to child pornography. The Optional Protocol to the Convention of the Rights of the

---

[41] Convention on Cybercrime, Explanatory Report (n 30) para 93.

[42] For this argument, see also Susan W Brenner, 'The Council of Europe's Convention on Cybercrime' in Jack M Balkin and others (eds), *Cybercrime: Digital Cops in a Networked Environment* (New York University Press 2007) 212.

[43] For this debate, see Miriam F Miquelon-Weismann, 'The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?'(2005) 23 *John Marshall J of Computer & Information L* 329, 354.

Child on the Sale of Children, Child Prostitution and Child Pornography does not deal specifically with the use of computer systems but contains, in Article 2(c) a sufficiently broad definition of child pornography: 'any representation, *by whatever means*, of a child engaged in real or *simulated* explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes'.[44] Few additional content-related offences appear in other multilateral instruments. The League of Arab States Convention goes beyond the criminalization of child pornography and requires States parties to criminalize the 'production, display, distribution, provision, publication, purchase, sale, import of [all] pornographic material' (art 12), with offences involving child pornography carrying increased punishment. The AU Convention contains similar provisions as the Budapest Convention with respect to child pornography and also demands that States criminalize computer-related acts involving racism and xenophobia (art 29(3)).

Finally, the Budapest Convention contains offences related to the infringements of copy-right and related rights (art 10). No particular conduct is defined; instead, the Convention refers to domestic law and the obligations undertaken by States pursuant to a number of international instruments in this area, such as the Bern Convention for the Protection of Literary and Artistic Works and the Copyright Treaty of the World Intellectual Property Organization. However, as Article 10(1) clarifies, the provision is intended to cover only those infringements that are committed 'wilfully' and 'on a commercial scale'.

Clearly, these offences do not encompass all possible cybercrimes. As the Explanatory Report to the Budapest Convention states, '[t]he list of offences included represents a minimum consensus not excluding extensions in domestic law'.[45] By way of example, the use of computers and computer systems to commit theft and extortion or to engage in other harmful activities, such as cyberstalking, are not covered. One may wonder why only some of the crimes already criminalized at the domestic level, such as forgery, fraud and child pornography, are included in the Budapest Convention, but not others.

Given that around 80 per cent of all cybercrime acts are committed through some form of organized activity,[46] another international instrument that can be relied upon to some extent in the fight against cybercrime is the United Nations Convention against Transnational Organized Crime from 2000 (Palermo Convention).[47] This treaty has been ratified almost universally, which makes it a potentially useful instrument to coordinate the global fight against cybercrime. Most cybercrimes can be subsumed under the definition of 'transnational' as defined in Article 3(2) of the Convention, according to which an offence is transnational when it is: (a) committed in more than one State; (b) committed in one State but planned, prepared, directed or controlled in another State; (c) committed in one State but involving an organized group engaging in criminal activities in more than one State; or (d) committed in one State but has substantial effects in another State.

---

[44] Optional Protocol to the Convention of the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, 25 May 2000, 2171 UNTS 227 (entered into force 18 January 2002) (emphasis added).

[45] Convention on Cybercrime, Explanatory Report (n 30) para 34.

[46] Expert Group to Conduct a Comprehensive Study on Cybercrime, 'Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector' (UNODC/CCPCJ/EG.4/2013/2, Vienna, February 2013) para 5.

[47] United Nations Convention against Transnational Organized Crime, 15 November 2000, 2225 UNTS 209 (entered into force 29 September 2003).

However, the Palermo Convention is only applicable to 'serious crimes', which are defined as 'conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty' (art 2(b)) and which are committed for the purpose of obtaining a financial or other material benefit (art 1(a)(i)); to the laundering of proceeds of a crime (art 6); and to corruption (art 8). In other words, even though the Palermo Convention is completely silent on cybercrime, certain serious forms of cybercriminal activities, such as organized online fraud, may well be covered by it.[48]

3. THE INTERNATIONAL REGIME TO FIGHT CYBERCRIME

The international regime to not only criminalize but fight cybercrime is equally dominated by the Budapest Convention which has been ratified by numerous countries in which the internet and the cybereconomy have a central place. The Convention seeks, as is the classical way of international criminal law, to enhance cooperation between member States. Among other things, States must be prepared to order and obtain 'the expeditious preservation of specified computer data' (art 16) and to ensure 'the expeditious disclosure … of traffic data' (art 17). Stored computer data may be searched and seized by the competent State authorities (art 19); traffic data may be collected or recorded (art 20), and content data intercepted (art 21), either by the authorities themselves or by compelling a service provider.

These provisions are not necessarily innovative when compared to existing international criminal law instruments. However, the Convention clearly attempts to deal with the particular volatility of computer data by adapting existing procedural law to the internet age, with the objective of allowing the competent authorities to proceed as rapidly as possible.[49] It is worth noting that, according to Article 19, the powers to search and seize are limited to the State's respective territory, which means that any transboundary search or seizure must follow the ordinary channels of mutual legal assistance.[50]

The powers and procedures referred to in Articles 16–21 are subject to a provision on 'conditions and safeguards' (art 15), according to which States must ensure the protection of human rights and liberties, for instance via judicial supervision. These rights include those protected under international law, such as by the European Convention on Human Rights (ECHR) and the International Covenant on Civil and Political Rights. However, as the Explanatory Report notes, it is left to the '[n]ational legislatures … to determine, in applying binding international obligations and established domestic principles, which of the powers and procedures are suffi-

---

[48] The only reference to computers is made in the provision on training and technical assistance, which requires States to initiate, develop or improve specific training programmes, including '[m]ethods used in combating transnational organized crime committed through the use of computers, telecommunications networks or other forms of modern technology'; ibid., art 29.1(h).

[49] The Convention, therefore, emphasizes expeditiousness, for instance of the preservation and disclosure of computer data. As the Explanatory Report notes, '[s]peed and, sometimes, secrecy are often vital for the success of an investigation.' Convention on Cybercrime, Explanatory Report (n 30) para 133.

[50] Ibid., para 195. The only exception is access to data that is publicly available or if the consent of the person who has the lawful authority to disclose the data has been obtained. Convention on Cybercrime (n 14) art 32.

ciently intrusive in nature to require implementation of particular conditions and safeguards'.[51] The Convention itself does not offer any specific procedural guarantees of due process.[52]

Interestingly, the Convention goes beyond its provisions on substantive law and requires all States to adopt measures to establish procedures for the purpose of criminal investigations or proceedings not only for the offences contained in the Convention but also for 'other criminal offences committed by means of a computer system' and 'the collection of evidence in electronic form of a criminal offence' (art 14(2)b and c).

The Budapest Convention also contains a number of provisions on mutual assistance and extradition that follow the overarching principle according to which the parties 'shall co-operate with each other … to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence' (art 23). Again, the provisions are drafted with the fact in mind that computer data may easily be deleted and is often stored for only short periods of time.[53] In addition to the possibility of relying on 'expedited means of communication, including fax or e-mail' (art 25), States parties must also designate a 24/7 point of contact to provide immediate assistance and be able to proceed, for instance, with an expedited preservation or disclosure of computer data (art 35). With respect to extradition, and similar to other instruments dealing with transnational crime such as the Palermo Convention, there is an *aut dedere aut judicare* requirement in the Budapest Convention, meaning that States must either extradite or bring the case before their own national authorities according to the principle (art 24(6)).

Other instruments contain similar provisions with respect to extradition and mutual legal assistance, including mechanisms for expedited assistance. While the AU Convention only touches on principles of international cooperation in a general manner and encourages States parties to sign the Convention on mutual legal assistance (art 28), the League of Arab States Convention contains detailed provisions on extradition and mutual assistance (arts 30–43). By way of example, States parties may be requested to seize, secure or disclose data in their territory, including through expedited means of communication, such as e-mail, and every State party is required to establish a 24/7 contact point 'to ensure the provision of prompt assistance' (art 43).[54] The League of Arab States Convention also resembles the Budapest Convention with respect to grounds for refusal of assistance. A State party may notably not respond to another State's request, for instance to preserve or disclose data, if 'the request concerns an offence which the requested Party considers a political offence' or if 'the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests'.[55] Although grounds for refusal should, generally speaking, be

---

[51] Convention on Cybercrime, Explanatory Report (n 30) para 147.

[52] For a critique of the lack of procedural guarantees, see Miquelon-Weismann (n 43) 341.

[53] See Convention on Cybercrime, Explanatory Report (n 30) para 256.

[54] For a discussion of institutional aspects and a few examples of ways in which such contact points were established, see Council of Europe, 'The effectiveness of international co-operation against cybercrime: examples of good practice', discussion paper prepared by Pedro Verdelho (12 March 2008) 21–4 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf.

[55] Convention on Cybercrime (n 14) arts 27(4), 29(5), 30(2); the corresponding provision in the League of Arab States Convention can be found in art 35.

'narrow and exercised with restraint',[56] it does not seem that detailed reasons must be specified if requests for assistance are refused by invoking one of these provisions.

In sum, the Budapest Convention represents a traditional, decentralized criminal law approach based on the territoriality principle of regulation and enforcement that seeks to increase the capacity of States to deal with cybercrimes. As Susan W Brenner has argued, cybercrime is treated in the Convention 'as an internal threat which is to be dealt with by the criminal justice system of a nation whose citizens have suffered 'harm' from a particular activity'.[57] The very fact of criminalizing similar behaviour in similar terms is in itself a great boost to transnational judicial cooperation, particularly in the extradition domain where the dual criminality rule typically requires that an offence exist in both the requesting and requested State.

4. THE PROBLEM OF JURISDICTION[58]

Crime is traditionally understood to be a largely territorial phenomenon, one in which 'the perpetrator(s) and victim(s) are all physically present at a specific geographical point when a crime is committed'.[59] At first glance, cybercrime challenges that framework in a very radical way, almost to the point of making 'geography irrelevant'.[60] Cybercrimes are often transnational, even global in their concrete operation, and not simply as a result of political fiat as in the case of major supranational crimes (genocide, crimes against humanity or war crimes may, after all, be quite national in character).

Having said that, and although cyberspace cannot easily be subsumed under traditional conceptions of a State's sovereignty over land, sea and air,[61] there is always a certain physicality even to cybercrime. Criticizing a common trope in the scholarship, for example, Orin S Kerr has argued that overreliance on 'virtual metaphors will obscure rather than illuminate the dynamics of computer crime. … what matters is the physical reality of the network, the actual bits and bytes, rather than the virtual world a user might imagine'.[62] At any rate, both prescriptive and adjudicative/enforcement issues arise that at the very least complicate issues of jurisdiction.

At the prescriptive level, in the 1980s and 1990s, several countries, especially in North America and Europe, started to adopt national legislation criminalizing certain cybercrimes. Since websites can usually be accessed in every country, the content of each website could be seen as having to comply with the national regulations of every country from where it

---

56 Convention on Cybercrime, Explanatory Report (n 30) para 268.
57 Brenner (n 42) 210.
58 For a general overview of jurisdiction in cyberspace, see Kohl (Ch 4 of this Handbook).
59 Susan W Brenner, 'Cybercrime Jurisdiction' (2006) 46 *Crime, L and Social Change* 189.
60 Ibid.
61 Bantekas (n 27) 135.
62 Orin S Kerr, 'Virtual Crime, Virtual Deterrence: A Skeptical View of Self-help, Architecture, and Civil Liability' (2005) 1 *J of L Economics and Policy* 197, 199–200. Kerr criticizes three proposals associated with virtual metaphors: offensive self-help strategies or 'cybervigilantism', 'architecture regulation', and civil liability for third-party computer operators.

was accessible.[63] The danger of overregulation, amplified in its complexity by a still highly fragmented system based on national legislation, is tangible. However, it stands to be limited through a practice of prescriptive jurisdiction hewing closely to the actual enforcement jurisdiction. As Uta Kohl highlights, the:

> fact that the existence of enforcement jurisdiction tends to be perceived as a prerequisite for exercising adjudicative/legislative jurisdiction in respect of transnational criminal activity means that the subjective territoriality principle, i.e., the country-of-origin approach, is far more user-friendly for States. … the person responsible for the acts tends to be on the State's territory.[64]

In terms of adjudication and enforcement, even if bolstered by mutual legal assistance treaties and extradition treaties, domestic laws are insufficient to establish jurisdiction over many cybercrimes and deal effectively with jurisdictional conflicts, especially in the case of cybercrimes of the latest generation. It is evident that the territoriality principle, one of the principles on which national criminal jurisdiction is usually based, is only of limited use in the context of cybercrime.[65] There may be no single *locus delicti* in the traditional sense; several offenders may act together yet from different locations; experienced crackers can route their activities through portals in jurisdictions without specific legislation; and digital evidence may be dispersed on servers located in different jurisdictions.

In most instances, however, the offenders, the victims and the harm caused are very real. Basing jurisdiction on the principle of nationality and of objective territoriality allows States both to prosecute and to seek to protect their own nationals. The principle of objective territoriality allows States to exercise jurisdiction over a conduct having a substantial effect in its territory, although the conduct occurred outside its territory. It is evocative of forms of protective jurisdiction more broadly. This approach is, for instance, adopted by the Budapest Convention. While the provisions on territorial jurisdiction are not very precise in this regard, with Article 22(1)(a) only requiring a State party to adopt measures allowing it to establish jurisdiction for offences committed 'in its territory', the Explanatory Report specifies that an offence committed 'in its territory' includes, for instance, the attack of a computer system in its territory, even if the attack is launched from outside its territory.[66]

Should the State of origin and the State of destination both be able to exercise jurisdiction? Conflicts are inevitable when the specific conduct in question is criminalized in the former but not in the latter. These conflicts can be negative (no State claims jurisdiction) or positive (multiple States do), both of which are potentially problematic. The Budapest Convention deals with this dilemma to some extent by allowing States, under Article 22(2), to opt out from the requirement to exercise jurisdiction over offences committed by a national if the offence is punishable where it was committed.[67] While integrating the general principle of *aut dedere*

---

[63] For this debate, see Uta Kohl, *Jurisdiction and the Internet* (CUP 2007) 24–6. For the argument that the rise of jurisdictional conflicts has been facilitated by technical developments, especially those relating to the territorial restriction of websites, see ibid., 104.

[64] Ibid., 106.

[65] For this argument, see also Fausto Pocar, 'New Challenges for International Rules Against Cyber-crime' (2004) 10 *European J on Criminal Policy and Research* 27, 36.

[66] Convention on Cybercrime, Explanatory Report (n 30) para 233.

[67] Convention on Cybercrime (n 14) art 22(1)(d). On negative and positive jurisdiction conflicts, see De Hert, Gonzáles Fuster and Koops (n 22) 519; see also Susan W Brenner and Bert-Jaap Koops, 'Approaches to Cybercrime Jurisdiction' (2004) 4 *J of High Technology L* 1.

aut judicare,[68] the Convention nonetheless provides little guidance to resolve jurisdictional conflicts and to avoid competition among law enforcement authorities. It merely states that: 'when more than one Party claims jurisdiction … the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution' (art 22(5)). These consultations are not mandatory and, as the Explanatory Report specifies, may even be declined if a State deems them an obstacle to its investigations.[69]

Compared to the Budapest Convention, the EU Framework Decision is more specific with respect to conflicts of jurisdiction. Relying above all on the territoriality and the nationality principles, three options, in order of preference, are outlined to determine which member State should prosecute: where the offence has been committed; whose national has committed the offence; and where the offender has been found.[70] The League of Arab States Convention also establishes a clear order of priority. When several States claim jurisdiction, the order is as follows: States whose security or interests have been disrupted; then States in whose territory the offence was committed; and finally, the State of the nationality of the offender (art 30(3)). In practice, it appears that States resolve jurisdictional conflicts on an ad hoc basis through formal and informal consultations.[71] As the UN Office on Drugs and Crimes has noted, 'forms of territoriality-based and nationality-based jurisdiction are almost always able to ensure a sufficient connection between cybercrime acts and at least one State'.[72]

5. CHALLENGES

Three areas seem to require specific attention in any attempt to deal with cybercrime: the role of service providers; the impact on rights; and the possibility of non-criminal preventive measures. First, regarding the regulation of the internet more generally, and the prevention of, and fight against, cybercrime more specifically, establishing the liability and responsibility of service providers, which are 'effectively the gatekeepers of data on the Internet',[73] may be particularly relevant. Moreover, law enforcement authorities increasingly seek the cooperation of private companies, such as information and service providers.[74] Several States have established requirements to retain data for a certain period and to disclose data following a formal request from law enforcement authorities.[75] The Budapest Convention only deals with internet service providers in a few procedure-related provisions, allowing, for instance, State authorities to compel service providers to collect or record data.[76] Several model legislative

---

[68] The provisions on extradition include the following clause:
If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Convention on Cybercrime (n 14) art 24(6).

[69] Convention on Cybercrime, Explanatory Report (n 30) para 239.

[70] See also De Hert, Gonzáles Fuster and Koops (n 22) 519.

[71] UN Office on Drugs and Crime (n 19) 189.

[72] Ibid.

[73] Clough (n 4) 8.

[74] Cristos Velasco, 'Cybercrime Jurisdiction: Past, Present and Future' (2015) 16 *ERA Forum* 331.

[75] UN Office on Drugs and Crime (n 19) 144–6.

[76] Convention on Cybercrime (n 14) arts 20(1)b and 21(1)b.

texts establish more extensive responsibilities, for instance, of access and hosting providers, including monitoring obligations.[77]

Second, the fight against cybercrime may have an impact on the human rights of users of computers and the internet, perhaps especially when service providers are enlisted in an enterprise of surveillance.[78] Although cybercrime is a concern for the public, the potential of cybercrime laws being interpreted by governments in ways that allow them to better suppress dissent or control populations is high, in ways that are very reminiscent of debates surrounding the repression of terrorism. The right to privacy may be violated, as may freedom of expression be unduly limited by content-related restrictions.[79] Concerns have been voiced that the Budapest Convention was established thanks to the work of a Committee of Experts with little access for civil society organizations, especially those concerned with privacy. It should be recalled that the Convention recognizes States' quite broad powers to combat even those cybercrimes that are not actually defined in it. Although the Preamble states that signatories are 'mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights', it does not itself establish guarantees to respect such rights, leaving it instead to the States parties to legislate on proportionality and checks and balances according to already existing obligations under human rights law. This means that no shared minimal standards with respect to due process exist for all States parties to the Budapest Convention.

Most notably, the ECHR, which may provide particularly useful guarantees in the context of the fight against cybercrime, is only applicable to the European States which are parties to this Convention; contrary to the Cybercrime Convention, the ECHR is not open to non-States parties of the CoE.[80] Moreover, there are no provisions in the Convention outside the Preamble on the protection of personal data, a sensitive issue in light of States' extensive surveillance powers and the fact that judicial cooperation under the Convention may lead to data being shared with States beyond those bound by the CoE's relatively protective standards.

More generally, the fight against cybercrime has created concerns that it may impair citizens' ability and right to 'seek, receive and impart information'[81] in a context where States may feel empowered to seize or otherwise obtain computer data without warrants or adopt

---

[77] E.g. the 2010 Model Legislative Texts on Cybercrime/e-Crimes and Electronic Evidence elaborated by the International Telecommunication Union (ITU)/Caribbean Community (CARICOM)/ Caribbean Telecommunications Union (CTU) and the 2011 Cybersecurity Draft Model Bill of the Common Market for Eastern and Southern Africa (COMESA).

[78] See Fidler (Ch 7 of this Handbook).

[79] Joint Declaration on Freedom of Expression and the Internet by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information, http://www.osce.org/fom/78309. The Joint Declaration states, for instance, that '[c]ontent filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression' (para 3.b). For a general discussion of human rights and cyberspace, see Ch 6 in this volume.

[80] For this discussion, in particular with reference to the US and decisions of the Supreme Court concluding that the ECHR and other international human rights instruments, such as the International Covenant on Civil and Political Rights, do not create enforceable rights in the US, see Miquelon-Weismann (n 38) 355–9.

[81] This is the language adopted by the 1948 Universal Declaration of Human Rights in art 19.

expansive libel laws when it comes to the internet.[82] However, combating cybercrime should arguably be subject to particular regulation. Just as some forms of cybercrime, because of their novel characteristics, demand specific legal responses, some of these responses may represent a particular threat to human rights. In other words, the potentially far-reaching intrusion into the lives of internet users, facilitated by automated surveillance and data storage, ought to be an inherent aspect of any initiatives intended to fight cybercrime.

Third, criminal law is obviously not the only avenue to combat cybercrime. A document entitled 'cybercrime report' of a software security producer is clearly not intended to promote criminal law responses to cybercrime but to make the online user protect herself through technical means. Indeed, when confronted with – increasingly automated – cybercrimes, we almost instinctively look for a technical defence: anti-virus programs, spam filters, firewalls, passwords, more secure online payment systems. Preventive measures are no doubt important and may have even more of a role in this field than in other areas of crime control.

Because of the typically transboundary nature of cybercriminal activities, cybercrime prevention, such as awareness-raising campaigns,[83] should also go beyond national boundaries, in particular in order to respond to emerging threats. Educating users to make them vigilant and take essential security precautions can eliminate many opportunities for cybercriminal activities. Although many potential offenders will use more sophisticated tools to act or find users located in places with a generally lower level of cybersecurity, the overall crime rate is likely to drop. Moreover, the private sector, notably service providers and software producers, plays an important role, which is why self-regulation, which may be highly effective, and the sharing of best practices ought to be encouraged and facilitated.[84]

Compared to this ready-to-use and easily adaptable arsenal and its more immediate and tangible impact, attempts to strengthen the transnational legal framework to combat cybercrime may look relatively removed from the site of crimes and ill adapted to prevent them. Technical responses, however, only deal with the effects and not with the underlying problem itself. In this sense, legal responses have the potential to have a more profound impact on criminal behaviour. Investigating and prosecuting cybercrimes in order to terminate a specific conduct, such as spamming, should thus not be weighed against the effectiveness of technical avenues. Criminal law is complementary to security measures[85] and has an inherent, if not easily measurable, deterrent effect.

---

[82] This was, for instance, the case of the highly controversial 2012 Cybercrime Prevention Act of the Philippines that extended criminal libel to the internet and provided for harsh prison sentences; the Act was suspended by the Supreme Court. For more information on the 2012 Act, see Human Rights Watch, 'Philippines: New "Cybercrime" Law Will Harm Free Speech' (28 September 2012) http://www.hrw.org/news/2012/09/28/philippines-new-cybercrime-law-will-harm-free-speech.

[83] For examples of such campaigns organized by governments and the private sector, see UN Office on Drugs and Crime (n 19) 234–6.

[84] E.g. Joint Declaration on Freedom of Expression and the Internet (n 79) para 1.f.

[85] The CoE Explanatory Report recognizes that '[t]he most effective means of preventing unauthorised access is, of course, the introduction and development of effective security measures. However, a comprehensive response has to include also the threat and use of criminal law measures'. Convention on Cybercrime, Explanatory Report (n 30) para 45.

6. CONCLUSION

It appears that all initiatives, whether at the national, regional or international level, only react – with a significant delay – to rapidly evolving forms of cybercriminal activities. It is of course difficult to conceive how law could anticipate future threats, in other words do more than *react* and *respond*. Cybercrime also reveals some of the shortcomings of the traditional State-based approach in the field of criminal law: the monopoly of power has largely become an illusion. States will undoubtedly need to develop more creative responses. Enhancing harmonization of substantive law and transnational cooperation via instruments like the Budapest Convention is certainly useful,[86] but several challenges remain, in addition to the Convention's provisions being susceptible to different interpretations by its States parties. More comprehensive approaches that integrate a deeper understanding of the functioning of information technology may be required.

In this sense, the emergence of entirely virtual worlds has already created a renewed need for theorizing about criminal law. Is stealing a virtual object in a virtual world a crime akin to theft?[87] Is virtual child pornography the same as the real thing? On the one hand, surely killing a virtual avatar is not identical to murder, even though it may be portrayed as such in a game environment. Some have argued for a relatively light intervention of the criminal law, leaving governance and disciplining of virtual spaces to their organizers. On the other hand, economic and social harms may occur as a result of actions occurring entirely in virtual spaces, not to mention the way in which such spaces may serve to play out or experiment with criminal behaviour in ways that may well spill over into the real world.

A key question is to what extent we can or should look beyond traditional criminal law responses and whether cybercrime requires radically new approaches. Is international law, and the law more generally, ill-equipped to deal with it? Additional options to strengthen existing and adopt new national and international legal responses to cybercrime, as identified by a United Nations Office on Drugs and Crime report in 2013,[88] include the development of international model provisions on the criminalization of cybercrimes, inter alia, to eliminate 'safe havens'; and the strengthening of cooperation in order to deliver enhanced technical assistance to combat cybercrime in developing countries. Furthermore, suggestions such as the establishment of an International Cybercrime Court or for the expansion of the competences of the International Criminal Court over cybercrimes[89] may be premature but have been voiced strongly.

The principle of universality merits consideration in this context. Traditionally, universal jurisdiction has been reserved for the arguably most serious crimes, including genocide and

---

[86] For an assessment, see Jonathan Clough, 'A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation' (2014) 40 *Monash University Law Review* 698.

[87] Andrea Vanina Arias, 'Life, Liberty, and the Pursuit of Swords and Armor: Regulating the Theft of Virtual Goods' (2007) 57 *Emory L J* 1301; Brenner (n 10); Brian Simpson, 'What Happens Online Stays Online? Virtual Punishment in the Real World' (2011) 20 *Information & Communications Technology L* 3.

[88] UN Office on Drugs and Crime (n 19).

[89] Stein Schjolberg, 'Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrime: An international criminal tribunal for cyberspace (ICTC), A Paper for the EastWest Institute (EWI) Cybercrime Legal Working Group' (2012) https://www.cybercrimelaw.net/documents/ICTC.pdf.

crimes against humanity. No traditional jurisdictional link being required, any State may exercise jurisdiction over such crimes, even if committed outside its territory by a non-national against non-nationals. It seems unlikely that a consensus regarding universal jurisdiction over cybercrime will develop anytime soon seen only through this prism; most cybercriminal activities do not 'shock the consciousness of humanity'[90] to the same degree as the crimes under the jurisdiction of the International Criminal Court. It might be conceivable, however, to imagine the application of the principle of universal jurisdiction on a basis closer to its original application to crimes of piracy, as a result of their occurring in areas that are beyond the jurisdiction of any State. Jurisdiction would be limited to a restricted list of the most serious cybercriminal activities that are universally condemned, in which case the State assuming jurisdiction would not need to establish a nexus according to the conventional criteria of territoriality or nationality. However, the threshold is likely to be high; the mere fact that an activity is deterritorialized in nature – as many cybercrimes are – cannot be considered an automatic justification for any State asserting jurisdiction.

In sum, cybercrime has not yet altered the nature and modalities of international law, with the current international legal responses rather following traditional approaches that were already evident in other areas of transboundary criminal law, such as human trafficking or drug trafficking. Various existing multilateral initiatives are valuable, since they lay the groundwork for greater cooperation between States. However, these instruments certainly further the risk of creating regional clusters and may create openings for hegemonic capture. It should also be noted that transnational criminal law is increasingly at risk of being overtaken, as a modality of dealing with the problem of cybercrime, with an emphasis on cybersecurity that circumvents some of the perceived cumbersomeness of even ameliorated criminal justice approaches or fuses them with potentially complex implications.[91] Global cooperation, beyond State or regional boundaries, and across the State/non-State divide, will remain necessary to deal with many forms of cybercrime.

---

[90] Rome Statute of the International Criminal Court, 17 July 1998, UN Doc A/CONF.183/9, preamble.

[91] Pauline C Reich, 'Cybercrime, Cybersecurity, and Financial Institutions Worldwide' in Takashi Kubota (ed), *Cyberlaw for Global E-business: Finance, Payments and Dispute Resolution* (IGI Global 2008); Nir Kshetri, *Cybercrime and Cybersecurity in the Global South* (Springer 2013); Stein Schjolberg and Solange Ghernaouti-Helie, 'A Global Treaty on Cybersecurity and Cybercrime' (2011) https://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf; Tatiana Tropina and Cromac Callanan, *Self-and co-regulation in Cybercrime, Cybersecurity and National Security* (Springer 2015).

13. The notion of cyber operations

Paul A. L. Ducheine and Peter B. M. J. Pijpers[1]

1. INTRODUCTION

The aim of this chapter is to elaborate on the notion of 'cyber operations' as they seem to be used in a generic manner in popular media as well as in academics.

This chapter differentiates between actors and motives, covering operations conducted by both State and non-State entities. Special attention will be paid to governmental cyber operations that are characterised by five distinct roles and paradigms: governance; protection; law enforcement; intelligence; and military operations. In addition, governmental response mechanisms, based on the paradigms, are explained and operations themselves are operationalised.

Despite similarities regarding means and methods used in all these cyber operations, the fundamental distinction lies in the purpose of those launching these activities. For governmental actors, the purposes are vested in the aforementioned paradigms.

1.1 Apples and Pears? No, Just (Different) Goals!

The concept of cyberspace, some 35 years ago coined by William Gibson,[2] can be understood as 'to cover all entities that are or may potentially be connected digitally'.[3] Ever since the activities executed within this cyber domain have often been framed in belligerent terms associated with conflict and attack, implying a malign nature full of warlike threats. But let us put this in context both for State and non-State entities.

Cyberspace is not merely used for malign purposes. In fact, most activities have a benign character related to commercial and private uses of the internet and social media. Moreover, various assessments reveal that it is digital espionage and cybercrime that have been, and

[1] The authors are grateful for the comments delivered by Prof Terry Gill, Mark Roorda, Willem van Poll and Dr Jelle van Haaster.

[2] William Gibson, *Neuromancer* (Penguin Press 2018).

[3] See Netherlands Defence Cyber Strategy (2012) (English Version): 'Cyberspace is understood to cover all entities that are or may potentially be connected digitally. The domain includes permanent connections as well as temporary or local connections, and in all cases relates in some way to the data (source code, information, etc.) present in this domain'. Original: *Parliamentary Papers II 2011-2012*, 33 321, No. 1.

remain,[4] the biggest threats to governments and the business community rather than 'cyber war'.[5]

The 2013 Snowden files have shed light on the covert activities of governmental intelligence agencies around the world conducting operations in and through cyberspace.[6] This appears self-evident for public (or governmental) agencies, however, the number of private enterprises digitally collecting and providing information is growing steadily.[7] Activities of intelligence agencies and private companies include social-media monitoring,[8] digital investigation,[9] and ordinary market research. Most notably, large ICT-companies such as Google, Microsoft and applications like Facebook, WhatsApp, Twitter, Instagram, Zoom and LinkedIn are also collecting data for (future) business purposes.[10] Google's knowledge of search-queries enables it to know more details about individuals than these people know (or realise) themselves.[11] This data can be utilised to micro target customers into persuading them to purchase products (i.e., marketing), for investigative journalism (i.e., Bellingcat),[12] to monitor Coronavirus lockdown rules,[13] but the same techniques are also used to sway voter preferences.[14] Since a number

---

[4] National Cyber Security Centre, 'Cyber Security Assessment Netherlands' (CSAN-1 2019) 7. These national assessments are confirmed by findings of others: Stephen Doherty and others, 'Hidden Lynx – Professional Hackers for Hire' (Symantec) https://www.wired.com/images_blogs/threatlevel/2013/09/hidden_lynx_final.pdf; Booz, Allen and Hamilton, 'The Logic Behind Russian Military Cyber Operations' (March 2020) https://www.boozallen.com/c/insight/publication/the-logic-behind-russian-military-cyber-operations.html.

[5] Thomas Rid, 'Cyber War Will Not Take Place' (2012) 35 *Journal Of Strategic Studies* 5.; John Stone, 'Cyber War Will Take Place!' (2013) 36 *Journal of Strategic Studies* 101.

[6] For the description of cyberspace used in this chapter, using a model with three dimensions (cognitive, virtual and physical) and sub-divided in seven layers consisting i.e., social groups, psyche, cyber-identities, cyber-objects, hardware, objects and geographical locations (of all entities). See Paul AL Ducheine and Jelle van Haaster, 'Fighting Power, Targeting and Cyber Operations' (2014) *International Conference on Cyber Conflict, CYCON*, 303; Paul AL Ducheine, Jelle van Haaster and Richard van Harskamp, 'Manoeuvring and Generating Effects in the Information Environment' (2017) 155.

[7] For instance, services provided by Information Security firms, see Mandiant's Intelligence Centre https://www.fireeye.com/mandiant.html, well known for reporting on China's alleged Advanced Persistent Threat, and the Dutch niche company Fox-IT www.fox-it.com/en.

[8] See *inter alia* https://www.coosto.com/en. Applications are offered for: Customer Service, Brand Monitoring, Campaign Monitoring, Crisis Monitoring, Competitor Monitoring and Data Research.

[9] See https://cyberinvestigationservices.com/, addressing Internet Defamation, Cyber Harassment, Hacking Investigation, and Cyber Security.

[10] Recently, a number of those companies advocated more restrictions on governmental surveillance and reform of legislation in this respect. See: www.reformgovernmentsurveillance.com.

[11] John Lancaster provokingly argues that Google, by virtue of its data, 'doesn't just know you're gay before you tell your mum; it knows you're gay before you do'; John Lanchester, 'The Snowden Files: Why the British Public should be Worried about GCHQ', *The Guardian* (3 October 2013) http://www.theguardian.com/world/2013/oct/03/edward-snowden-files-john-lanchester .

[12] Bellingcat Investigation Team, 'MH-17 Archive', https://www.bellingcat.com/tag/mh17.

[13] Elizabeth Beattie, 'We're Watching You : COVID-19 Surveillance Raises Privacy Fears', *Al Jazeera* (2020) https://www.aljazeera.com/news/2020/4/3/were-watching-you-covid-19-surveillance-raises-privacy-fears

[14] Carole Cadwalladr, 'Exposing Cambridge Analytica: "It's Been Exhausting, Exhilarating, and Slightly Terrifying"', *The Guardian* (29 September 2018) https://www.theguardian.com/membership/2018/sep/29/cambridge-analytica-cadwalladr-observer-facebook-zuckerberg-wylie; Emma Graham-Harrison, Carole Cadwalladr and Hilary Osborne, 'Cambridge Analytica Boasts of Dirty Tricks

of these ICT companies are being observed by, collaborate with or are forced to work with governmental intelligence agencies, this private (and economic) information is likely also available for the latter.

Beyond espionage and intelligence, the other substantial threat originates from a group of actors that bear no public responsibility at all: criminals who use cyberspace as a vector for their actions, as a target for their activity, as a line of communication, or as a marketplace to sell their 'products' on the so-called dark web.[15] In order to counter this threat, stakeholders varying from individuals to Internet Service Providers, from anti-virus vendors to governments, have taken a variety of countermeasures. These measures may be preventive in nature by installing firewalls and anti-virus software, by penalising cybercrime by implementing the Budapest Cybercrime Convention,[16] or through participation in the UNODC supported workgroup on preventing and combatting cybercrime.[17] In addition, governments are preparing responses by drafting legislation enabling law enforcement officials to 'hack-back', once designated forms of (cyber) crime have been discovered.[18]

However, apart from espionage and crime, cyberspace is also used for a variety of other malicious purposes. According to David Sanger, the US and Israel produced and used the famous Stuxnet virus against nuclear production facilities in Iran, delaying its nuclear program and thereby biding time and preventing (or postponing) a physical (military) aka 'kinetic'

---

to Swing Election', *The Guardian* (19 March 2018) https://www.theguardian.com/uk-news/2018/mar/19/cambridge-analytica-execs-boast-dirty-tricks-honey-traps-elections; Alex Hern, 'Far More than 87m Facebook Users Had Data Compromised, MPs Told', *The Guardian* (17 April 2018) https://www.theguardian.com/uk-news/2018/apr/17/facebook-users-data-compromised-far-more-than-87m-mps-told-cambridge-analytica.

[15] Cybercrime activities of actors like Hansa Market and Silk Road are i.a. ransomware and malware attacks; crypto mining; stealing, leaking and manipulating data; trafficking; and violating privacy. See also: Andy Greenberg, 'Operation Bayonet: Inside the Sting That Hijacked an Entire Dark Web Drug Market', *Wired* (3 August 2018) https://web.archive.org/web/20180308164513/https:/www.wired.com/story/hansa-dutch-police-sting-operation/; Nicole Hong, 'Silk Road Creator Found Guilty of Cybercrimes', *Wall Street Journal* (4 February 2015) https://www.wsj.com/articles/silk-road-creator-found-guilty-of-cybercrimes-1423083107.

[16] 65 States have ratified the Budapest Convention, 44 as member of the Council of Europe and 21 Third Party members. See also: Kubo Mačák, Laurent Gisel and Tilman Rodenhauser, 'Cyber Attacks against Hospitals and the Covid-19 Pandemic: How Strong Are International Law Protections?' (27 March 2020) *Just Security*,https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/.

[17] Council of Europe, Convention on Cybercrime 2001; UNODC, 'Group of 77 Workshop on Preventing and Combating Cybercrime supported by the Russian Federation and the United Nations Office on Drugs and Crime' (218).

[18] See *inter alia*: Michiel van Blommestein, '"Hack back" law would let Dutch police install spyware, eavesdrop on Skype', *ZDNet* (3 May 2013) http://www.zdnet.com/hack-back-law-would-let-dutch-police-install-spyware-eavesdrop-on-skype-7000014867/; and Peter Sommer, 'Police Powers to Hack: current UK law' (2012) 18 *Computer and Telecommunications Law Review* 165; Jan-Jaap Oerlemans, 'Oversight of Hacking Power and Take down Order' (12 October 2017) *LeidenLawBlog*, https://leidenlawblog.nl/articles/oversight-of-hacking-power-and-take-down-order .

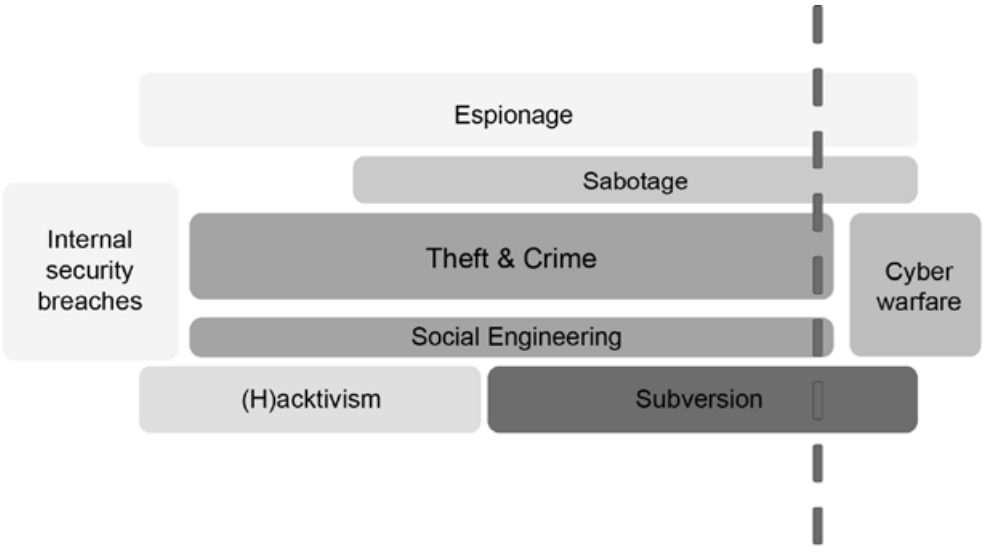


Figure 13.1 Cyber threat landscape

operation against Iran's nuclear program.[19] This form of cyber sabotage or 'cybotage',[20] was a complicated, multidimensional and costly operation against an Industrial Control System (ICS) not connected to the Internet and therefore physically protected by (inter alia) a so-called 'air gap'. This, however, did not hamper the operation and might become even more likely since researchers have now evidenced that acoustic signals may also cross air gaps like these.[21] Hence, cyber activities have had effects in the physical domain, and will have, with reference to the 2015 and 2016 sabotage of the Ukrainian power grid.[22]

Finally, cyberspace also features and supports warfare, war-related activities and (other) military operations. In 2007, Syrian air defences did not notice Israeli jets bombing a nuclear facility at al Kibar; apparently, the air defences were manipulated from outside, using cyberspace as an entrance and digital code as tooling.[23] During the Second Gaza War (2012), Israel Defence Force (IDF) and Hamas were battling in cyberspace, using blogs and tweets as instru-

[19] David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (Crown 2012) 188 *ff*; David Sanger, *The Perfect Weapon : War, Sabotage, and Fear in the Cyber Age* (Scribe 2018) Chapter 1.

[20] John Arquilla, 'Cyberwar Is Already Upon Us - But can it be controlled?', *Foreign Policy* (27 February 2012) http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us #sthash.OfFAFk4W.dpbs.

[21] Michael Hanspach and Michael Goetz, 'On Covert Acoustical Mesh Networks in Air' (2013) 8 *Journal of Communications* 758.

[22] Robert Lee, Michael Assante and Tim Conway, 'Analysis of the Cyber Attack on the Ukrainian Power Grid' (18 March 2016) *SANS Industrial Control Systems Security Blog*, Report available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2016/12/21181126/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[23] Peter Warren Singer and Allan Friedman, *Cybersecurity and Cyberwar - What Everyone Needs to Know* (OUP 2014) 126–8.

ments in an information campaign.[24] Sympathisers (or victims) expressed their feelings and ideas as well.[25] Characteristic for cyberspace, geographical dislocation does not hamper groups and individuals from joining conflicts (and other forms of social behaviour), thus confronting or supporting the warring parties digitally.[26] Hackers bearing the name Anonymous, launched their '#OpIsrael', defacing and obstructing Israeli websites and e-services,[27] or declaring 'war' against ISIS and taking control of hundreds of ISIS Twitter accounts.[28] Thus, Anonymous and (h)activist groups alike have entered the realm of conflict,[29] partially in pursuance of their 'corporate' mission, but by launching virtual (i.e., cyber) operations, also entering the domain of operations that are closely related to the physical military conflict that is being fought by the warring factions as well.

Cyber operations as displayed above are executed by both State and non-State entities. Though the objectives may differ, the activities are similar, varying from digital espionage; criminal and subversive acts including DDoS-attacks, hacking and leaking operations, defacements and destruction of data; up to acts that have an effect in the physical world, be that in war or situations short of war.

Whichever source is behind these threats, irrespective of the motivation that is driving such cyber activities, and regardless where and against what or whom they are conducted or directed, the common denominator of these forms of social behaviour, seems – at first glance – to be a military and warlike one, as all of them are referred to as 'attacks', the activities quite often labelled as 'operations', and the total once and again is characterised as 'cyber warfare', making comparisons with the Cold War[30] or refer to an arms race in cyberspace,[31] as if the whole phenomenon were militarised.

---

[24] Tweets from @IDFSpokesman and on the IDF–website, e.g., https://twitter.com/idf or https://www.idf.il/en/articles/hamas/how-is-the-idf-minimizing-harm-to-civilians-in-gaza/. IDF communication on Hamas in general: https://www.idf.il/en/minisites/hamas//. Hamas operatives' use of Twitter can be found on twitter.com/AlqassamBrigade, for instance with https://twitter.com/AlqassamBrigade/status/269186182225747968/photo/1/large, the account was suspended by Twitter, see 'Twitter suspends English account of Hamas military wing', *Al Arabiya News* (12 January 2014) http://english.alarabiya.net/en/media/digital/2014/01/12/Twitter-suspends-English-account-of-Hamas-s-military-wing-.html; Lily Hay Newman, 'What Israel's Strike on Hamas Hackers Means For Cyberwar', *Wired* (6 May 2020) https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/.

[25] For instance, occupiedpalestine.wordpress.com/2012/11/18/gazaunderattack-nov-18-2012-live-blog/ (this website includes graphic images that readers may find disturbing).

[26] Gabriella Coleman, 'Anonymous in Context: The Politics and Power behind the Mask', *International Governance Innovation* (2013) http://www.cigionline.org/sites/default/files/no3_8.pdf.

[27] Anonymous, '#OpIsrael' (2012) http://www.youtube.com/watch?v=q760tsz1Z7M.

[28] Alex Hern, 'Anonymous "at War" with ISIS, Hacktivist Group Confirms', *The Guardian* (17 November 2015) https://www.theguardian.com/technology/2015/nov/17/anonymous-war-isis-hacktivist-group-confirms; Alex Hern, 'Islamic State Twitter Accounts Get a Rainbow Makeover from Anonymous Hackers', *The Guardian* (17 June 2016) https://www.theguardian.com/technology/2016/jun/17/islamic-state-twitter-accounts-rainbow-makeover-anonymous-hackers.

[29] I.e. in the factual meaning, without necessarily (direct) participation in the hostilities.

[30] Herbert Lin, 'The Existential Threat from Cyber-Enabled Information Warfare' (2019) 75 *Atomic Scientists* 187, 190.

[31] Veronika Netolicka and Miroslav Mares, 'Arms Race "in Cyberspace" – A Case Study of Iran and Israel' (2018) 37 *Comparative Strategy* 414, 415–6.

1.2 The Military in Cyber?

However, despite the belligerent language often used,[32] in reality, the portion of military involvement in cyber activities seems fairly limited. This, yet, ought to be nuanced. This observation may be true regarding cyber warfare proper, i.e., the conduct of military cyber operations in the context of an armed conflict in the legal meaning.[33] Yet, as cyber operations may not – and most times do not – qualify as cyber warfare proper, other cyber operations are characterised by military involvement as well. Therefore, the military's contribution to cyber operations is larger: quantitatively and qualitatively.

First of all, the military portion may be larger in numbers (quantity), as some States have provisions whereby the military are involved through non-military institutional arrangements. Some of the military intelligence and security services operate under civil (i.e., non-military) legislation and control. Some of the intelligence services have a dual role: civil and military tasking alike. In addition, some States have a role for military police forces within the law enforcement domain.

Secondly, although small in numbers, the military may play a crucial and inevitable role in providing 'cyber security'. Nowadays, governments increasingly rely on a multidisciplinary or inter-agency approaches to (modern) security threats as is clearly visible in counter-terrorism and cyber-security policies, thus using the 'whole of government' to face and address modern threats.

Moreover, some States have decided that an active and forward presence in their digital defence with other (State and non-State) actors beyond the territorial boundaries of their own cyber-infrastructure cannot be executed without military assistance.[34] The purpose of this so-called 'persistent engagement' in cyberspace is the surveillance and monitoring of (potential) threats based on tacit agreed competition of cyber activities below the threshold of the use of force.[35]

1.3 Aim, Perspective and Structure

Suitable or not, the term cyber operation seems to become a common denominator for activities in cyberspace, undertaken with the aim of achieving objectives in or through this digital domain. The common denominator can be used in a great variety of situations, by a diversity of actors and, quite obviously, for various reasons.

The aim of this contribution is therefore to elaborate on this notion of 'cyber operations' as they seem to be used as a universal, a rather generic and non-specific term. As a starting point,

---

[32] Kenneth Watkin, 'The Cyber Road Ahead: Merging Lanes and Legal Challenges' (2013) 89 *International Law Studies* 472, 503.

[33] See, e.g., Terry D Gill and Paul AL Ducheine, 'Anticipatory Self-Defense in the Cyber Context' (2013) 89 *International Law Studies* 438.

[34] United States Cyber Command, 'Achieve and Maintain Cyberspace Superiority' (2018) 1, 3–5; Jason Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace' (2019) 5 *Journal of Cybersecurity* 1, 9.

[35] Michael P Fischerkeller and Richard J Harknett, 'Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace' (9 November 2018) *Lawfare*, https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

the definition offered by the Tallinn Manual's international group of experts will be used for this purpose. Cyber operations are defined as: 'The employment of cyber capabilities [with the primary purpose of] achieving objectives in or through cyberspace'.[36]

The primary perspective will be that of the State, the principal subjects of international law.[37] However, as demonstrated above, since non-State entities are on par in this domain or even exceed States in activities, attention will also be paid to the characteristics of cyber operations conducted by non-State actors.

Although not all non-State actors may have explicitly formulated a formal strategy as States (normally) do, some will have an implied, rudimentary articulated 'corporate goal or end'.[38] Whether communicated explicitly or not, and regardless of its legitimacy, State and non-State actors alike allocate resources (means) and undertake activities (ways) in order to achieve those designated goals or ends.[39] In doing so, both non-State actors (at least rational ones) and States use strategic objectives at the 'corporate' or 'strategic' level of their organisation. These strategic objectives are subsequently implemented by subordinate entities at the operational (or tactical) level through the allocation of means, and the definition of ways to employ the latter. These two characteristics of organisations – objectives and means and methods – will be used to describe differences and similarities in the various cyber operations.

First, for State and non-State entities alike, the differences in objectives at the strategic level will be displayed (Section 2). Section 3 will then reveal similarities at the operational level, being the 'means and methods' used to achieve these strategic objectives.

Subsequently, the primary focus will be on State actors, displaying the distinct roles of States by articulating five strategic paradigms used to characterise cyber activities, their purposes and institutional frameworks (Section 4). Section 5 then operationalises cyber operations (in general) and military cyber operations in particular (Section 6) by describing its specific features and phases.

2. DIVERSITY IN STRATEGIC OBJECTIVES

States and non-State entities (at any rate lucid ones) alike will be inspired or driven by implied or publicly stated institutional (i.e., national or corporate) strategy. Even when ostensibly merely reacting to 'events', State and non-State activities will be driven or guided by (some basic form of) strategic imperative. This is also true for activities in cyberspace. These

---

[36] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) Glossary definition, 564. The addition 'with the primary purpose' is made by the authors, in reference to the 2013 Tallinn Manual on the International Law Applicable to Cyber Warfare.

[37] Robert Jennings and Arthur Watts, *Oppenheim's International Law*, vol I (Longman 1996) 16.

[38] On non-State actors' strategies, e.g., Lawrence Freedman, *Strategy - A History* (OUP 2013) 474 *ff*; and Peter R Neumann and MLR Smith, 'Strategic Terrorism: The Framework and its Fallacies' in Thomas G Mahnken and Joseph A Maiolo (eds), *Strategic Studies - A Reader* (Routledge 2008) 342. Some non-State actors have explicitly stated 'strategic objectives' e.g., Hamas' strategy as expressed in its Charter http://avalon.law.yale.edu/20th_century/hamas.asp; and The Syrian Electronic Army at https://deibert.citizenlab.ca/2011/06/syrian-electronic-army-disruptive-attacks-and-hyped-targets/#more-1422 (initially published on http://www.infowar-monitor.net, the website is no longer available).

[39] AIV and CAVV, 'Cyber Warfare (Report No. 77/22, 2011)', Advisory Council on International Affairs (AIV) & Advisory Committee on Issues of Public International Law (CAVV) 12.

strategic imperatives may be 'plain and simple', for instance economic profit, or complex, ranging from enhancing cyber security – as (*inter alia*) crucial and critical public and private infrastructure or services are reliant on ICT – to achieving military superiority in cyberspace.

The primary aim of States will be to enhance (national) security and to promote and safeguard their (other) vital national interests. These vital interests may be stated in a grand or national security strategy, or they may be implied in or deducted from national (security) policies,[40] some explicitly focussing on cyber security issues.[41] As cyberspace is interconnected with other domains, and vital interests are increasingly interrelated and dependant on ICT and digital networks e.g., the internet, security in cyberspace (hence cyber security) is a vital strategic interests in its own right (see Figure 13.2), as also alluded in the Netherlands National Security Strategy.[42] Examples of the inextricable connection between the vital interests in the digital domain is the hack into the Netherlands' Diginotar case.[43]

Looking at non-State actors, their strategic notion may differ from that of States and often originates from commercial or ideological incentives. Regarding legitimate commercial enterprises, their goal will be economic profit, as it is the case for Kaspersky, Norton, Symantec, Google, Facebook *et al*.[44] Of particular interest are commercial enterprises that appear to be

---

[40] See e.g., Executive Office of the President of the United States, 'National Cyber Strategy of the United States of America', https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; Ministery of Foreign Affairs of the People's Republic of China, 'International Strategy of Cooperation on Cyberspace', https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm; Australian Government Department of Foreign Affairs and Trade, 'Australia's International Cyber Engagement Strategy' (2017); Ministre de Europe et de Affairs Etrangeres, 'Stratégie Internationale de La France Pour Le Numérique' https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf; AIV and CAVV (n 39) 12.

[41] See for an overview of those States e.g.: Regner Sabillon, Victor Cavaller and Jeimy Cano, 'National Cyber Security Strategies: Global Trends in Cyberspace' (2016) 5 *International Journal of Computer Science and Software Engineering* 2409; OECD, 'Cybersecurity Policy Making at a Turning Point – Analysing a new generation of national cybersecurity strategies for the Internet economy' (2012) 66 *ff*, https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf; CCD COE, 'National Strategy and Governance' (NATO Cooperative Cyber Defence Centre of Excellence) https://ccdcoe.org/library/strategy-and-governance/; ENISA, 'National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace' (2012) https://www.enisa.europa.eu/publications/cyber-security-strategies-paper.

[42] Netherlands National Coordinator Terrorism & Security, 'National Security Strategy' (2019) 12 (stating that '[a]s national security can also be affected via cyberspace, cybersecurity has been interwoven into all of the other national security interests').

[43] Dutch Safety Board, *The DigiNotar Incident* (2018) 3-6. On the impact of the case, see National Cyber Security Centre, *Cyber Security Assessment Netherlands (CSAN)-3*, 18: 'For example IT, telecommunications and electricity are fundamental for the functioning of many (other) vital sectors and processes in society. Failure in any one of these sectors can result in damaging effects in all sectors'. But see also more recent cases i.a. the 5G discourse; Kate O'Flaherty, 'New 5G Security Threat Sparks Snooping Fears', *Forbes* (13 November 2019) https://www.forbes.com/sites/kateoflahertyuk/2019/11/13/new-5g-security-threats-spark-snooping-fears/#787cc72a5025.

[44] www.symantec.com/corporate_responsibility/topic.jsp?id=ceo_letter:

> Symantec's mission is to make the world a safer place by protecting and managing information so everyone is free to focus on achieving their goals. It's a statement that ties our business goals to a social purpose as we help people, businesses, and governments secure and manage their information-driven world against more risks at more points, more completely and efficiently than any other company.

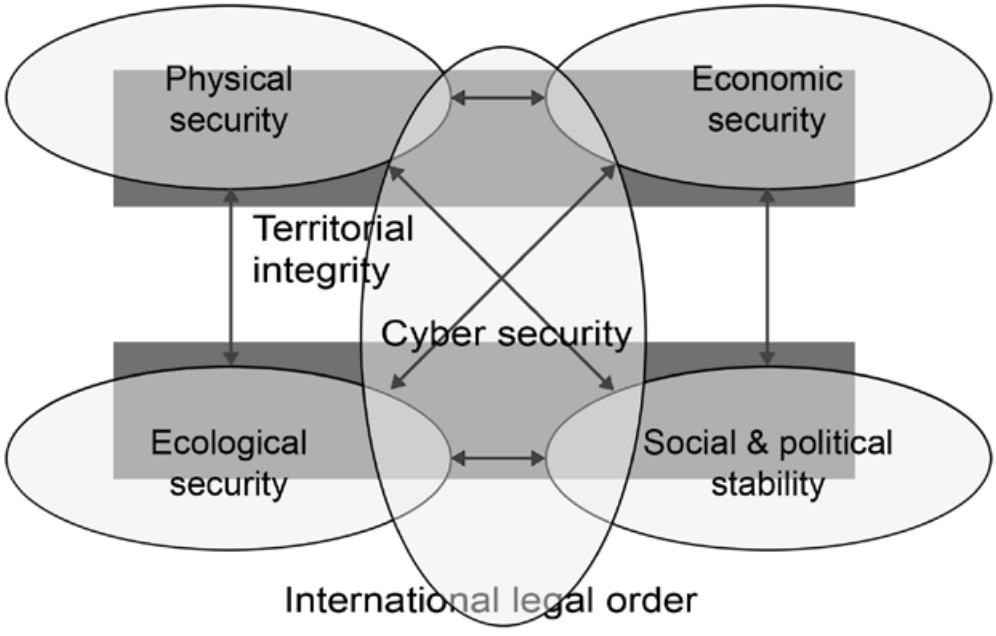


Figure 13.2 National security and its vital interests (for the Netherlands)

supplying tools enabling others to conduct cyber activities.[45] Cyber activities are part of their business model, if not their product.[46] Actors with a specific malign intent, such as hackers executing an Advanced Persistent Threats (APT) which can be cyber criminals seeking intellectual property or financial information, to State-controlled or proxy 'hackers for hire' stealing data or compromising cyber-infrastructure. Non-profit organisations such as Bellingcat, the TOR-project, Anonymous or CCC,[47] as well as thematic pressure groups such as Bits of Freedom, Privacy First or the Electronic Frontier Foundation will pursue political and/or ideological goals.[48] Their cyber activities will be more focussed on freedom of expression,

[45] E.g., the US based Palantir, at http://www.palantir.com/; the French company Vupen, the founders launched the firm Zerodium in 2015, https://www.zerodium.com; or Israeli enterprise Terrogence www.terrogence.com.

[46] https://www.fox-it.com/nl-en/who-we-are/; also 'Hold Security provides the best innovative services to meet your company's needs'; www.holdsecurity.com:

> It is Fox-IT's mission to make technical and innovative solutions that ensure a more secure society. We do that through the development of advanced cybersecurity and cyberdefense services and solutions for our clients around the world. We achieve this through a strong focus on innovation and a tireless dedication to our clients, our values, and our integrity.

[47] On Anonymous, see e.g., Coleman. See the German Chaos Computer Club or CCC, http://www.ccc.de/en/.

[48] E.g., 'Privacy First takes a professional and evidence-based approach to the various issues. The preservation of liberty in the private sphere can be perfectly combined with rapidly changing societal and technological developments'; www.privacyfirst.eu/. 'From the Internet to the iPod, technologies are transforming our society and empowering us as speakers, citizens, creators, and consumers. When our

transparency, free internet, net neutrality, privacy, etc. Cyberspace may be at the heart of their strategic values, or may offer leverage as a vector or medium for their activities.

Ideology also seems to be the primary objective of non-State actors that have entered battlefields and conflicts digitally: Hamas, Hezbollah, the Syrian Electronic Army, and again, Anonymous *cum suis*. Apart from ideology, some of these actors may also have other ambitions that may even resemble those of States: territorial or military. Recent events have demonstrated that non-State actors, with or without the sponsoring of affiliated States, have conducted numerous 'cyber operations' ranging from purely ideological (Estonia 2007; UK 2016, France 2017), in support of (or at least supportive to) military conflict (Georgia, 2008; Ukraine, 2014, 2015, 2016), autonomous (Anonymous, 2012) or as part of military conflict (Hezbollah, 2006; Hamas, 2012).[49] In more than one respect, their operations are quite similar to cyber operations conducted by States (through their organs), and as such, these operations are as instrumental to corporate strategic aims, as they are for States.

In sum, State and non-State cyber activities, regardless of their legitimacy and legality under national and international law, potentially pose threats to what is defined as cyber security.[50] When combined, these threats represent a threat landscape as depicted in Figure 13.1 above.

3. COMMON OPERATIONAL MEANS AND METHODS

Although the strategic objectives of the various actors conducting cyber operations may differ, in general they use the same capabilities in terms of means and methods.[51] This is demonstrated by the shared dependency on knowledge and skills that is required to conduct these activities. Thus, whether operating in governmental service (military and civil), commercial companies, pressure or activist groups, or in sheer isolation, all cyber operators or 'hackers' – white, grey and black hats alike – require the same skills and expertise.

Apart from personnel, knowledge and skills as a prerequisite for cyber capabilities, the ways and capacities, or in other words, the means and methods to achieve strategic aims are comparable. All cyber actors will require similar (if not the same) tooling, software and hardware, whether it is their intent to provide legitimate services, to prevent misuse of cyberspace, or because misuse is their very goal. One of the clearest demonstrations of commonalities at the operational level vis-à-vis cyber means and methods is monitoring software (and hardware) that is used by CERTs, intelligence agencies, law enforcement official, military units, civilian cyber security companies, as well as organised criminal groups or hacktivist groups.

However, they may take opposing sides. Taking into account that the aims of cyber-security companies (e.g., Symantec) and vendors (e.g., Microsoft) on the one hand, and cyber criminals on the other hand will be opposite, their 'business-models' or in other words, the operational ways to achieve goals, centre on the same lines of software and code. Where it is Symantec's

---

freedoms in the networked world come under attack, the Electronic Frontier Foundation (EFF) is the first line of defense': https://www.eff.org/about.

[49] For an update on cyber operations, see: https://www.cfr.org/interactive/cyber-operations.

[50] Cybersecurity is 'the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes'. See: Cisco Systems, *What is Cybersecurity?* https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

[51] AIV and CAVV (n 39) 15, 17 and 36.

and Microsoft's task to discover and/or to fix vulnerabilities, it is the criminal's intent to exploit these very weaknesses.

Thus, despite strategic differences between States and (some) non-State actors, at the operational (and tactical) level, there appears to be more similarity as all actors – conceptually – rely on more or less the same basic requirements (personnel, knowledge and skills) and means and methods, that is: capabilities and capacities (see Section 5).

With this conclusion in mind, the next sections will take a State perspective as a starting point in order to further differentiate between the varieties of cyber operations.[52]

4. APPLICABLE CYBER PARADIGMS FOR STATES

Looking at cyber activities at the State level, a number of distinct paradigms are applicable to describe cyber operations: coordination and governance, protection, law enforcement, intelligence and military operations.[53]

These paradigms are demonstrated in national cyber security strategies worldwide,[54] as well as through the instrumental use of cyber capabilities in furtherance of States' (other) vital interests.[55] These paradigms – related to the inherent governmental function to provide security and to further vital interests of the State – can be depicted as parts of a continuum, a spectrum, or to put it differently, as part of a State's comprehensive efforts in cyberspace.[56] The paradigms are complementary and overlapping.[57]

These paradigms represent one (or more) of the institutional frameworks enabling governments (or public authorities) to conduct activities within democratic societies. They thus offer a legal and social framework for (governmental) behaviour that is, as with all social interaction, subject to adjustments that are initiated or inspired by changes in the security landscape (including 'new' threats), public opinion, international, societal and technological trends. As such, these frameworks reflect the *Zeitgeist* regarding topics that have reached the political agenda and require or enable governmental action.[58]

In democratic States, adhering to the principle of the rule of law, these arrangements and organisations, at least when exercising public authority (that may interfere with civil liberties), will have a designated legal basis establishing the organisations and arrangements in the very first place. In addition, these arrangements and organisation will have to execute their tasks and powers in accordance with legal regimes that are applicable once these activities are conducted. The designated legal bases and legal regimes, together with oversight mechanisms,

---

[52] When and where required, special attention will be paid to non-State actors conducting cyber operations, criminal activities excluded, although the analysis offered may fit their activities as well.

[53] See also: Alexander Klimberg and Philipp Mirtl, 'Cyberspace and Governance—A Primer' Austrian Institute for International Affairs http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/Cyberspace_and_Governance_-_Working_Paper_65_2.pdf 15.

[54] For an overview: see footnote 40.

[55] E.g., Stuxnet. For a discussion see references at n 19.

[56] AIV and CAVV (n 39) 16

[57] Klimberg and Mirtl (n 53) 15 (referring to these paradigms as 'mandates').

[58] On the process of 'securitization' in the digital domain, e.g., Maarten Rothman and Theo Brinkel, 'Of snoops and pirates: Competing discourses of cybersecurity' in Paul AL Ducheine, Frans Osinga and J Soeters (eds), *Cyber Warfare: Critical Perspectives* (TMC Asser Press 2012) 49.

authority and accountability rules, are part of the legal framework that characterises the various paradigms.

The frameworks can be understood as the product of existing (inter)national law, political systems, political attention, public opinion, public demands, as well as (lack of) audacity and leadership. The frameworks are tangible through (institutional and ad hoc) arrangements and governmental organisations tasked with designated roles in cyberspace and cyber security.[59]

The rise of these frameworks and paradigms, is evident when analysing States' cyber security policies or strategies. Five core paradigms can be detected: coordination and (internet) governance including diplomacy; protection; law enforcement; (counter) intelligence;[60] and military operations which include conflict (see Figure 13.3).[61] They will be explored subsequently below.

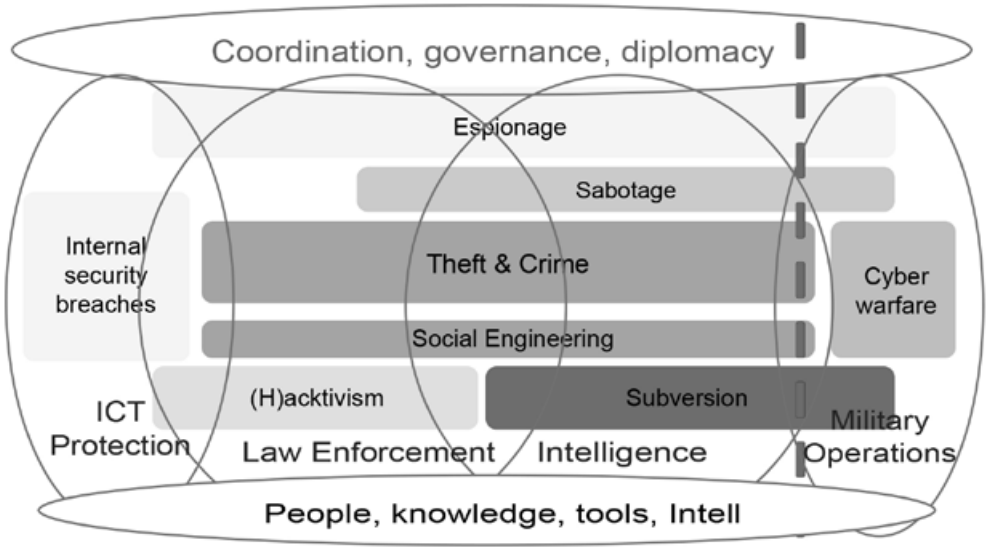


Figure 13.3 Cyber security paradigms

Each of these paradigms provides a framework that represents public support, legal bases, legal regimes, and institutional arrangements. More than often, these frameworks are used in a complementary manner. Taken together they enable cyber operations throughout a wide and fluid spectrum, ranging from 'the monitoring of governmental networks by Computer Emergency Response Teams or CERTs, to active protection by shutting down sites once they are under 'attack', and followed by 'criminal investigations into the source of the "attacks"

[59] Eric Luiijf and Jason Healey, 'Organisational Structures & Considerations' in Alexander Klimburg (ed), *National Cyber Security Framework Manual* (CCD COE 2012) 109–10.

[60] Including counter-security.

[61] See also: Paul AL Ducheine and others, 'Towards a Legal Framework for Military Cyber Operations' in Ducheine, Osinga and Soeters (n 58) 110.

where criminal activity was reasonably suspected'.[62] These operations may be combined with 'intelligence operations to *inter alia* ascertain the nature of the threat posed and identify the source of the threat, possibly resulting in a military response in situations which rose to the level of a use of armed force by a foreign power or organised armed group, even resulting, in exceptional cases, in participation in an armed conflict'.[63]

4.1 Coordination, Governance and Diplomacy

Although this framework does not comprise actual cyber activities, coordination first of all refers to internet governance,[64] diplomacy[65] and to national and international efforts to shape (governance in) the digital domain.[66] As cyberspace – unlike physical domains – is characterised by a dominant role for non-State actors, both private and non-governmental,[67] the role of States is thus different compared to the physical world, and to a certain extent rather limited,[68] although not irrelevant.[69] The added value of States in this domain lies, *inter alia*, in the use of 'classic' instruments such as bilateral or multilateral treaties,[70] cooperation,[71] as well as in their position in governmental and non-governmental bodies such as the EU,[72] UN[73] or ITU.[74] Secondly, coordination refers to national coordination between the public and private organisations contributing to the other four paradigms. Agencies such as the French ANSSI, the UK's GCHQ or the Netherlands' NCSC have a coordinating role directing governmental

---

62 As, for instance, in counter-terrorism, see ibid., 110.

63 Ibid.

64 For a definition of internet governance see: WSIS, 'Tunis Agenda for the Information Society (WSIS-05/TUNIS/DOC/6(Rev. 1)-E) (2005)' (ITU 2005) para 34, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

65 Heli Tiirmaa-Klaar, 'Cyber Diplomacy: Agenda, Challenges and Mission' in Klimburg (n 59).

66 Jovan Kurbalija, 'E-Diplomacy and Diplomatic Law in the Internet Era' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy* (CCD COE 2013).

67 Laura DeNardis, *The Global War for Internet Governance* (Yale University Press 2014) 1–2.

68 Luiijf and Healey (n 59) 127.

69 ICANN, 'Who runs the internet?' (2013) http://www.icann.org/en/about/learning/factsheets/governance-06feb13-en.pdf; Ian Walden, 'International Telecommunications Law, the Internet and the Regulation of Cyberspace' in Ziolkowski (n 66).

70 E.g., Convention on Cybercrime.

71 E.g., NATO's efforts through its cyber defence policy, NATO, 'Chicago Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012' (2012) http://www.nato.int/cps/en/SID-8DB5C229-B80F4E08/natolive/official_texts_87593.htm?selectedLocale=en.

72 E.g., EU Cyber Direct, 'Cyber Diplomacy in the European Union' (2019).EU, 'A Digital Agenda for Europe (COM(2010) 245 final/2)' (2010) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF.

73 E.g., UN GGE 2017 Report, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A /72/327' (2017) 13985; UN General Assembly, 'Resolution on Establishment of OEWG - A/RES/73/72' (5 December 2018); UN General Assembly, 'The right to privacy in the digital age (UN Doc. GA/11475)' (19 December 2013). http://www.un.org/News/Press/docs//2013/ga11475.doc.htm.

74 ITU, 'Global Cybersecurity Agenda' (2007) https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx. See e.g., the World Summit on the Information Society (WSIS) declarations and outcome documents: Geneva 2003 (Geneva Declaration of Principles and Geneva Plan of Action) and Tunis 2005.

departments, and advising and guiding private actors. It is fair to say that State activities in the field of internet governance are pro-active and preventive in nature,[75] and are part of States' overall cyber security interests and strategies.[76]

4.2 Protection

The second paradigm for State activities in the cyber domain is related to the protection of (critical) cyber infrastructure.[77] In part this refers to 'ordinary' critical infrastructure such as electricity or waterworks as far as this infrastructure is connected with or processed through cyberspace. Originally, critical infrastructure protection (CIP) refers to, primarily, physical protection against accidents, disasters, technical or human failure, and crime.

In addition, vulnerabilities in the digital domain itself, referring to the logical layer, may be the focal point of (in)security issues, regardless of whether these breaches had a technical or human trigger, or whether they are the result of accidental or deliberate events. Serious cyber incidents may lead to major disturbances and disruption of society.[78]

But the protection of infrastructure also entails deliberate violations due to remote cyber-attacks resulting in damage or the loss of functionality of the infrastructure.[79] Cyber incidents in Estonia (2007), the spread of the Stuxnet virus (2010) but also the (Not)Petya (2016/2017) and WannaCry (2017) attacks have had a direct or indirect effect on CIP as well. Since many of the critical or vital services and installations are controlled through or depending on cyberspace, security in the digital domain is becoming ever more important.[80]

Protection as a paradigm refers to a range of State activities, varying from resilience, redundancy, to prevention (legislation, imposing incentives for 'hardening', physical protection, firewalls, DMZs, and technical standards) all the way to countering security breaches. The establishment of Information Sharing and Analysis Centres (ISACs) and CERTs is just one of the examples. Looking at the nature of the critical infrastructure and that of cyberspace in particular, it is evident that public-private cooperation is a prerequisite for States in order to ensure effective (implementation of) cyber security policy.

Of particular interest is the issue of 'governance' in protective perspective. Various ideas, i.e., 'notice and take down', have been proposed and criticised, demonstrating the delicate equilibrium in the public-private domain as these ideas require support from essential private partners.[81] However, over time, responsible disclosure policies, and even mandatory

---

[75] Luiijf and Healey (n 59) 129.

[76] E.g., The Netherlands' National Cyber Security Centre, *National Cyber Security Strategy - 2 From awareness to capability* (2013) 10, http://wwwenisaeuropaeu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversiepdf: 'The Netherlands aims to develop a hub for expertise on international law and cyber security'. See e.g., the involvement in the UNGGE and OEWG, UN General Assembly, 'Resolution on establishment of OEWG - A/RES/73/72' (5 December 2018); UN General Assembly, 'Resolution of establishment of UN GGE - A/RES/73/226' (22 December 2018).

[77] Protection is thus one perspective in order to promote the wider notion of overarching 'security'.

[78] On a critical note however, e.g., Sean Lawson, 'Beyond Cyber-Doom: Cyber Attack Scenarios and the Evidence of History (reprint)' in Ducheine, Osinga and Soeters (n 58) 277.

[79] Tallinn Manual 2.0 (n 36) rule 4, 20–1.

[80] The Stuxnet-virus was designed to infect a so-called Industrial Control System (ICS) that was not connected with internet.

[81] See e.g., the policy of the British Library (a non-departmental public body): http://www.bl.uk/aboutus/terms/notice/.

reporting of breaches (in vital sectors) and through privacy related mechanisms have been enacted.[82] Although some legal and legislative issues are covered by other paradigms (e.g., law enforcement and military operations) it is fair to say that the role of protective powers and countermeasures is not as sophisticated in cyberspace as they are in other domains. To date, more than once, States have enacted legislation empowering private security companies in the *physical* world to provide armed services.[83] Security is thus – once more – no longer the exclusive domain of State actors. As mentioned above, some commercial enterprises are rather active in cyberspace as well. Internet service providers (ISPs) and other digital services alike, play a pivotal role in this paradigm as well. Where consumers and organisations (small and large) fail to secure their ICT systems in an effective manner, these services are at the front of fighting spam, malware or unauthorised intrusions.[84]

Though protection is defensive in nature, a more active posture is chosen by some States, based on the postulation that cyberspace is inherently hostile. According to this stance, it is required to increase resilience, defend beyond the limits of national infrastructure and persistently engage with State and non-State entities acting in a similar way.[85] Despite its terminology, this stance does not seem to fit well in the 'protection paradigm'. From its content, the stance probably uses a combination of the law enforcement, intelligence and even military operations paradigm too.

However, apart from the other arrangements related to the law-enforcement, intelligence or military operations paradigm, State and private contractors usually lack powers to actually execute cyber operation from a protective perspective. Interestingly though, these powers frequently have been made available in the realm of physical security, for instance in the field of guarding military infrastructure.[86] Paradoxically, Dutch military guards may thwart an attack against physical military infrastructure, even with the use of lethal force,[87] whereas the Dutch Defence CERT is not empowered to use digital force to repel or stop cyber-attacks against MoDs digital infrastructure and data, including networks. Until now, such defensive measures, or to put it alternatively, cyber operations, would be the exclusive realm of other paradigms such as law enforcement or intelligence.

4.3 Law Enforcement

Law enforcement is (thus) one of those alternative paradigms for States, providing for preventive measures by penalising cybercrime, repressive measures by empowering law enforcement agencies to conduct investigations and so forth. The law enforcement paradigm

---

[82] See e.g., art 33 of the GDPR, https://gdpr-info.eu/art-33-gdpr/.

[83] E.g., in the field of counter-piracy: see Bibi van Ginkel, Frans-Paul van der Putten and Willem Molenaar, *State or Private Protection against Maritime Piracy? A Dutch Perspective* (Clingendael Centre for International Relations 2013).

[84] E.g., the ISP Code of Practice and the identification of compromised customer systems in Australia: Australian Attorney-General's Department, 'Cyber Security Strategy' (2009) http://wwwaggovau/RightsAndProtections/CyberSecurity/Pages/defaultaspx.

[85] United States Cyber Command (n 34) 6.

[86] See Ducheine and others (n 61) 114–5. For a European overview of such powers: Georg Nolte (ed), *European Military Law Systems* (de Gruyter Verlag 2003).

[87] Article 1 of the Act on the Use of Force by Guards of Military Objects (Staatsblad 2003) 134.

'comprises a wide set of organisations' at various levels, i.e., national and international,[88] local and national, and various governmental agencies and departments,[89] i.e., national police, EUROPOL, ministries of justice, internal affairs but also defence for military police; railway and traffic police.[90] To be effective, public-private partnership may be required, as well as cooperation with national (and other) CERTs and public-private ISACs, as well as intelligence and security services.

Apart from (harmonising and) penalising cybercrime, enforcement powers in the digital domain require amendments as well. To date, even 'classic' crime investigations heavily relies on digital investigative techniques, as physical pieces of evidence are increasingly superseded by digital ones.[91] When cybercrime is involved, additional enforcement and investigative powers will be essential to enhance effective policing and prosecuting.[92] Thus, States have enacted additional legislation, e.g., the Netherlands,[93] the UK[94] and others.[95]

As in any other domain, powers to execute cyber activities for law enforcement purposes, will require public support, at least political support, resulting in legislation providing a legal basis and applicable legal rules or a code of conduct (i.e., legal regimes). The legal framework is a common requirement derived not only from the principles of democratic States, but more in particular from obligations resulting from international human rights treaties or customary law.[96]

Apart from the delicate issues of balancing intrusive powers with human rights, especially privacy and freedom of expression, the other main dispute concerns the extra-territorial application of these law enforcement powers, e.g., when hacking back is used as a method by the

---

[88] Tiirmaa-Klaar (n 65) 520.

[89] Luiijf and Healey (n 59) 122 (referring to 'mandates' instead of paradigms).

[90] On the international legal dimensions of cyber crime see Kastner and Mégret (Ch 12 of this Handbook).

[91] For a plea to support amendments in this respect: https://www.hsleiden.nl/binaries/content/assets/hsl/lectoraten/digital-forensics-en-e-discovery/publicaties/2013/2013-breaking-the-backlog-of-digital-forensic-evidence---helpnetsecurity.pdf.

[92] Bert-Jaap Koops, 'Cybercrime Legislation in the Netherlands - Country report for the 18th International Congress on Comparative Law' (Washington, DC 25-31 July 2010) (session 'Internet Crimes' http://arno.uvt.nl/show.cgi?fid=107191).

[93] For the Netherlands: a preliminary draft of the proposal on Cyber Crime III was published in the beginning of 2013, see: Blommestein. The draft-proposal is due to be presented to Parliament in the beginning of 2014. The draft (in Dutch) can be found at: https://www.internetconsultatie.nl/computercriminaliteit/document/726.

[94] For the (rejected) UK amendment to the Regulation of Investigatory Powers Act (RIPA) 2000, see the Communications Data Bill at www.official-documents.gov.uk/document/cm83/8359/8359.asp. For US ideas: Dennis C. Blair and Jon M. Huntsman Jr., 'The IP Commission Report - The Commission on the Theft of American Intellectual Property (May 2013)' http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf; and on the Cyber Intelligence Sharing and Protection Act (CISPA): Electronic Frontier Foundation, 'CISPA is Back: FAQ on What it is and Why it's Still Dangerous' https://www.eff.org/cybersecurity-bill-faq.

[95] The Explanatory Note (Dutch: 'Memorie van Toelichting') to the Dutch preliminary draft proposal, refers to the situation in Belgium (Dutch: Wet inzake informatiecriminaliteit, Wet van 28 November 2000, Belgisch Staatsblad, 3 februari 2001, nr. 2909) France and Germany.

[96] On the protection of human rights in cyberspace see Fidler (Ch 7 of this Handbook).

police.[97] Public international law principles such as non-intervention and the sovereign rights of States will be major points of reference in this respect.[98]

4.4 Intelligence and Counter Intelligence

Apart from, and in addition to the law enforcement paradigm, States also rely on a classic security paradigm called intelligence (and counter intelligence), including espionage and countering security threats through intelligence and security organisations. Depending on institutional and constitutional arrangements, States have essentially similar tasking for their intelligence and security services. Their primary function is to gather and analyse information about threats directed against the State and its population.[99] This is based on, and in accordance with applicable law and political guidance. Collecting information in and through cyberspace is complementary to the existing set of capabilities being used by these services.[100]

After the terrorist assaults of 2001 (9/11), 2004 (Madrid) and 2005 (London), legislation has been amended (or at least drafted and proposed) to (more) effectively counter terrorist threats.[101] This legislation also includes powers (and regulations) to gather information (or intelligence) through cyberspace, hence cyber operations. Amendments and supplements to the legal bases for these powers and activities, have been the result of a successful attempt to use the window of opportunity after 9/11.[102] However, as a result of the joint revelations of whistle-blowers, journalists and activists, these powers and applicable regimes are up for public debate and legal review.[103] This public and political attention will remain of influence to

---

[97] E.g., the Dutch preliminary draft proposal refers – rather briefly – to this controversial issue by stating 'much will depend on the nature of the actual cyber enforcement activity [i.e. hacking back] whether or not public international law will legitimize the conduct of the law enforcement agencies' (translation by the authors).

[98] On non-intervention, sovereignty and counter-measures short of force, see respectively: Terry D Gill, 'Non-Intervention in the Cyber Context' in Ziolkowski (n 66); Benedikt Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace' in Ziolkowski (n 66); Michael N Schmitt, '"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law' (2014) 53 *Virginia Journal of International Law* 697, 700 *ff*. See further Roscini (Ch 14 of this Handbook).

[99] Aidan Wills, *Guidebook Understanding Intelligence Oversight* (2011) 11 https://www.dcaf.ch/guidebook-understanding-intelligence-oversight.

[100] Luiijf and Healey (n 59) 124.

[101] E.g., in the US, this involves the Patriot Act (2001), the Protect America Act (PAA) of 2007 and the FISA (Foreign Intelligence Surveillance Act) Amendment Act 2008 (FAA 2008). See: Joris van Hoboken, Axel Arnbak and Nico van Eijk, *Obscured by Clouds or How to Address Governmental Access to Cloud Data From Abroad* (2013) 5, http://www.ivir.nl/publications/vanhoboken/obscured_by_clouds.pdf.

[102] For an elusive oversight: Shane Harris, *@War: The Rise of the Military-Internet Complex* (Headline Publishers 2014).

[103] For an overview of the Snowdon revelations, supported by the lawyer-journalist Glenn Greenwald, Laura Poitras, and publications in the Guardian and Der Spiegel, see e.g., https//mailman.stanford.edu/pipermail/liberationtech/2014-January/012498.html. For the US report on these issues: Richard A. Clarke and others, *Liberty and Security in a Changing World - Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies* (2013) https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf; Glen Greenwald, *No Place to Hide - Edward Snowden, the NSA and the Surveillance State* (Penguin 2015) and Luke Harding, *The Snowden Files* (Vintage Publishers 2014).

(future) cyber operations and renew, *inter alia*, the debate regarding necessity, effectiveness, human rights and so on.[104]

Although most tasks for intelligence services are defensive in nature, a pro-active stance is also possible. Some States permit their intelligence services 'to exploit the information for other purposes, or directly intervene in order to prevent threats from (re)occurring'.[105] The earlier mentioned Stuxnet virus is probably one of the best-known cases in this respect. Actions undertaken by intelligence services to counter cyber threats – i.e., counter-intelligence – are a furtherance of those that can be found within the protective paradigm, or could be the start of a cyber operation that fits within the military (covert) paradigm.

Apart from national legislation, intelligence gathering is the subject of international legal attention as well.[106] Although no prohibition of cyber activities per se of cyber espionage exists in international law, it is clear the intelligence activities in or through cyberspace (cyber operations) may affect various national jurisdictions in a number of ways. In addition to the fact that the operations may qualify as criminal offences according to domestic criminal codes, they may also involve violations of civil law, international private law (intellectual property rights) and trade law.[107] Moreover, public international law may be implicated in a number of ways.[108] First of all, diplomatic law is of influence. But more importantly, some of the general principles of international law, i.e., State sovereignty, non-intervention as well as the prohibition on the use of force have an effect on the legal framework within this paradigm. Compared to classic intelligence activities, the extra-territorial dimension, and thus the international law ramifications are more pronounced as cyber infrastructure is situated in various jurisdictions and States.[109]

4.5 Military Operations and Conflict

The last – and in some respects the most extreme – of the five core paradigms for States is the one that could be characterised as military operations, including conflict.[110] The paradigm comprises (a) warfare proper (the conduct of military operations within the framework of

---

[104] E.g., Dinah PoKempner, 'Cyberspace and State Obligations in the Area of Human Rights' in Ziolkowski (n 66) 252.

[105] Luiijf and Healey (n 59) 124, referring to UK Cabinet Office, 'Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space' (25 November 2011) https://www.gov.uk/government/publications/cyber-security-strategy.

[106] On cyber espionage and international law see Buchan and Navarrete (Ch 11 of this Handbook).

[107] David P Fidler, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies' (2013) 17 *ASIL Insights* 1, 2. See generally on espionage and international law Simon Chesterman, 'The Spy Who Came in from the Cold War: Intelligence and International Law' (2006) 27 *Michigan Journal of International Law* 1071.

[108] Katharina Ziolkowski, 'General Principles of International Law as Applicable in Cyberspace' in Ziolkowski (n 66) 169; Pirker (n 98) 202; Gill (n 98) 224 *ff*; Ziolkowski, 'Peacetime Cyber Espionage – New Tendencies in Public International Law' in Ziolkowski (n 66) 425 ff.

[109] On cyber espionage see Buchan and Navarrete (Ch 11 of this Handbook).

[110] For reasons of clarity and for the purpose of this contribution, the author refrained from using 'warfare' in its more generic meaning: the art of conducting military operations (including i.a. warfare proper).

armed conflict) and (b) 'operations other than war' including peace support (and enforcement) operations related to conflict, but outside the framework of armed conflict.[111]

Military cyber operations, quite often referred to as 'cyber warfare' in its generic meaning, have been preliminary defined (see: Section 1) as the 'employment of cyber capabilities with the primary purpose of achieving [military] objectives in or by the use of cyberspace'.[112] These military objectives are translations of a State's strategic objectives. Apart from the present authors' specification, this definition is rather broad.

Other definitions are more specific, e.g., the Dutch Advisory Council on International Affairs (AIV) & Advisory Committee on Issues of Public International Law (CAVV), in their joint advice to the Netherlands Government, meaning: 'the conduct of military operations to disrupt, mislead, modify or destroy an opponent's computer systems or networks by means of cyber capabilities'.[113] This rather specific and enemy centric definition refers to three key criteria:

- the presence of a military operation aimed at achieving a political or military advantage,
- the causing of damage to the opponent's [sic] cyber infrastructure; and
- the use of cyber capabilities (since computer systems can also be destroyed using kinetic capabilities).[114]

The UK based Chatham House steers away from this enemy-centric definition and applies a more liberal – at least from a legal and law of armed conflict (hereafter: LOAC) point of view – characterisation, concluding that 'cyber warfare can enable actors to achieve their political and strategic goals without the need for armed conflict'.[115]

Taking note of contemporary military doctrine, the military – alongside economic power, diplomatic power and information – are comprehensively used as one of the instruments of State powers to achieve goals by influencing actors through the application (or threat) of 'fighting power'.[116] Hence, the actors to be influenced could be opponents or enemies, however, neutral actors will be encouraged to stay (at least) neutral or even persuaded to partner with the military, whilst supportive actors will be stimulated to remain supportive.[117] The military is thus instrumental to the State's strategic interests and goals, providing for

---

[111] For an illustrative summary of these operations, see Terry D Gill and Dieter Fleck, *The Handbook of the International Law of Military Operations* (OUP 2010).

[112] Michael N Schmitt (ed), *Tallinn manual on the international law applicable to cyber warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (CUP 2013) 258 (referring to this notion as 'cyber warfare').

[113] AIV and CAVV (n 39) 9 (also using 'cyber warfare').

[114] Ibid.

[115] Paul Cornish and others, *On Cyber Warfare* (Chatham House 2010) 37, http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf preceded by a definition:

> Cyber warfare can be a conflict between states, but it could also involve non-state actors in various ways. In cyber warfare it is extremely difficult to direct precise and proportionate force; the target could be military, industrial or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target.

[116] E.g., UK Ministry of Defence, *Joint Doctrine Publication 0-01 (JDP 0-01)* (4th Edition, 2011) 4–1, https://wwwgovuk/government/uploads/system/uploads/attachment_data/file/33697/20111130jdp001_bdd_Ed4pdf.

[117] E.g., Ducheine and Haaster, 'Fighting Power, Targeting and Cyber Operations' (n 6).

a number of strategic functions: anticipation, prevention, deterrence, protection, intervention, stabilisation, and normalisation.[118]

In conclusion, cyber operations are characterised by the employment of cyber capabilities with the primary purpose of achieving military objectives by influencing actors in or by the use of cyberspace.

The military operations paradigm in kinetic and cyber situations alike, provides an institutional framework guaranteeing social legitimacy (public support),[119] as well as legal legitimacy or legality:[120] a proper legal basis to launch operations,[121] and adherence to the applicable legal regimes for the conduct of operations.[122] As in any other military operation, an 'adequate' legal basis is required before it is decided upon and undertaken.[123] Legal regimes refer to those rules that are applicable once an operation commences.[124] One could think of the law of armed conflict, human rights law, and military codes.[125] In addition, though they do not qualify as 'law' proper, operational and political guidelines governing the use of force, known as Rules of Engagement (ROE), national caveats, or Tactical Directives et al are considered to be part of the 'legal regimes'. Both legal bases and legal regimes make up the legal framework for

---

[118] David Jordan and others, *Understanding Modern Warfare* (CUP 2008). E.g., Ministerie van Defensie, *Netherlandse Defence Doctrine* (2013) 37, http://wwwdefensienl/binaries/defensie/documenten/publicaties/2013/11/20/defence-doctrine-en/defensie-doctrine_enpdf. In a similar way: US Department of Defense, *Doctrine for the Armed Forces of the United States (Joint Publication 1)* (25-3-2013 edn, Joint Chiefs of Staff 2013) I–10 – I–11. UK Ministry of Defence, 1–8 – 1–11 – quoting Field Marshal Viscount Alanbrooke – uses the term Military Strategy, being the:

> art to derive from the [policy] aim a series of military objectives to be achieved: to assess these objectives as to the military requirements they create, and the pre-conditions which the achievement of each is likely to necessitate: to measure available and potential resources against the requirements and to chart from this process a coherent pattern of priorities and a rational course of action.

[119] The UK and Dutch doctrines use 'legitimacy' as an overarching framework: UK Ministry of Defence, 1–22: 'Legitimacy encompasses the legal, moral, political, diplomatic and ethical propriety of the conduct of military force'; and Ministerie van Defensie (n 118) 99: 'Legitimacy has a legal and an ethical side. Legal legitimacy primarily requires a legal basis for the mission. Secondly, legitimacy is based on the observance of rules that apply during the mission'.

[120] See Paul AL Ducheine and Eric H Pouw, 'Legitimizing the Use of Force: Legal Bases for Operation Enduring Freedom and ISAF' in Jan van der Meulen and others (eds), *Mission Uruzgan: Collaborating in multiple coalitions for Afghanistan* (Amsterdam University Press 2012) and Paul AL Ducheine and Eric H Pouw, 'Controlling the Use of Force: Legal Regimes' in Jan van der Meulen and others (eds), *Mission Uruzgan: Collaborating in multiple coalitions for Afghanistan* (Amsterdam University Press 2012), both available at: http://www.uva.nl/binaries/content/documents/personalpages/d/u/p.a.l.ducheine/nl/tabblad-twee/tabblad-twee/cpitem%5B8%5D/asset.

[121] This is normally a prerogative of the Executive branch, see: Sascha Hardt, Luc Verhey and Wytze van der Woude (eds), *Parliaments and Military Missions* (Europa Law Publishing 2012).

[122] Legal basis and legal regimes are covered by the denominator of 'legality': UK Ministry of Defence, 1–22.

[123] Ducheine and others (n 61) 112; Paul AL Ducheine, Kraesten L Arnold and Peter BMJ Pijpers, 'Decision-Making and Parliamentary Control for International Military Cyber Operations by the Netherlands Armed Forces' (2020) 184 56. On the use of force and international law see Roscini (Ch 14 of this Handbook).

[124] Some LOAC rules even apply before operations are launched: e.g., regarding the dissemination of LOAC and the employment of legal advisers.

[125] On human rights and cyberspace see Fidler (Ch 7 of this Handbook). Part IV of this Handbook deals with the application of the LOAC to cyberspace.

military cyber operations, covering the whole spectrum of (pro-) active, passive, offensive and defensive cyber operation.[126]

5. RESPONSE MECHANISM

The five core paradigms mentioned above – coordination and governance, protection, law enforcement, intelligence and military operations – all have different and unique legal and institutional frameworks, and aim for different effects to be achieved. But on the other hand, the paradigms do overlap, especially in the means and methods used and it must not be excluded that a government agency can operate in different paradigm under different legal coverage.

Furthering and protecting vital interests is not a one-way activity. Rivalling or opposing actors or audiences can take the initiative to act or can react to earlier engagements. Moreover, the cyber security paradigms can have a reactive, proactive or active stance. Democratic societies usually respond proportionally but that does not mean in kind or from within the same paradigm.

The most common legal bases for responses are retorsion, countermeasures, a plea of necessity and self-defence.[127]

In responding to a prior engagement, the utility of the paradigms is comprehensive within but also beyond cyberspace. An intrusive cyber operation breaching the sovereignty of a State can be answered with diplomatic means or with a hack-back by the protectors supported by a law enforcement legal base. A cyber armed attack can be retaliated with the use of force, both with cyber- but also kinetic means.

Cyber operations, whether initiated by the State, or in response to a prior engagement follow a certain sequence which will be described in section 6.

6. OPERATIONALISING CYBER OPERATIONS

As was evident from the description, the paradigms on the State level share many similarities related to common skills, knowledge, techniques and tactics, capacities, capabilities in other words in means and methods. Notwithstanding the obvious difference in objectives and its effects, a common model to (describe and thus) operationalise cyber operations is available. This descriptive six-phased model is useful in explaining the modus operandi of (a number of) cyber operations.[128]

Though the model itself may be helpful to understand cyber operations in general, it remains crucial to realise that the designated paradigm is of influence for the objectives of the opera-

---

[126] Ducheine and others (n 61) 112.

[127] See on Tallinn Manual 2.0 (n 36) rules 20–6, 111–38. On State responsibility and cyberspace see Antonopoulos (Ch 6 of this Handbook).

[128] See also similar models by Laura Galante and Ee Shaun, 'Defining Russian Interference : An Analysis of Select 2014 to 2018 Cyber Enabled Incidents' (2018) September Atlantic Council. < https://www.atlanticcouncil.org/wp-content/uploads/2018/09/Defining_Russian_Election_Interference_web.pdf> or Aristedes Mahairas and Mikhail Dvilyanski, 'Disinformation – (Dezinformatsiya)' [2018] *The Cyber Defense Review* 21, 24–5.

tions defined, and thus for the effects that are to be achieved through these operations.[129] The model comprises six phases that – in full or in part – may characterise and describe a typical cyber operation:[130]

- reconnaissance,
- design,
- intrusion,
- action,
- camouflage, and
- exfiltration.

Subject to the particular purpose of the operation, one or more of the phases can be expected. During an intelligence operation with the objective to scan the infrastructure of other actors, an initial operation may be limited to scanning ports, thus the operations will have one phase only: reconnaissance. With the information thus gathered, a more targeted operation may be designed to gather additional information on the hardware and software configuration of the actor's ICT system, encompassing all phases, with again an intelligence objective. Based on the collected information (taken together with other sources) a supplementary law enforcement operation could be started to gather forensic evidence, again going through all of the six phases. In addition, as a spin-off of the two operations, a designated military operation could be drafted as well, again using one of more of the phases described.

It will be evident that these three examples will be governed by their respective paradigmatic framework, including the legal frameworks. All three operations will require a legal basis, an objective (end), will need means (operators and tools), and will use methods requiring a plan, an addressee (or 'target'), techniques tactics and skills, all in accordance with the applicable legal regimes, and have oversight mechanism ensuring legitimacy and accountability.[131] For

---

[129] To some extent, activities and actors that haven't received detailed attention so far, e.g., cybercrime/criminals or hacktivism/hacktivists, 'follow' this model as well.

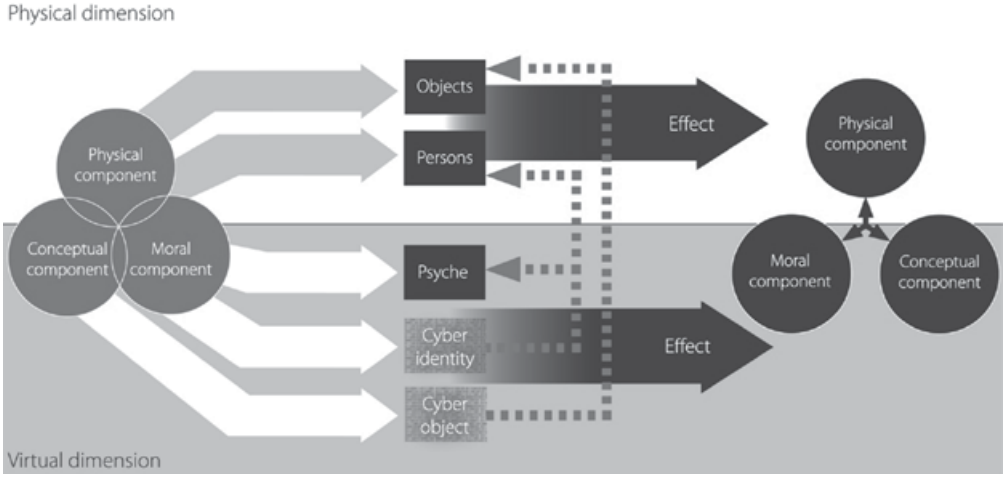
[130] Various descriptions are used, e.g., Paul Pols, 'The Unified Kill Chain' [2017] CSA Thesis, The Hague 1.https://www.csacademy.nl/en/csa-theses/february-2018/104-the-unified-kill-chain; Lech J Janczewski and Andrew M Colarik, *Cyber Warfare and Cyber Terrorism* (Information Science Reference 2008), 121, and Tom Olzak, 'The five phases of a successful network penetration' (2008) http://www.techrepublic.com/blog/it-security/the-five-phases-of-a-successful-network-penetration/701/; Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Syngress 2011) 171, using nine (plus one: obfuscating). Markus Maybaum, 'Technical Methods, Techniques, Tools and Effects of Cyber Operations' in Ziolkowski (n 65) 103, uses seven (based on Irving Lachow, 'Active Cyber Defence – A Framework for Policymakers'; http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf. This concept was originally presented in Eric M Hutchins, Michael J Cloppert and Rohan M Amin, 'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains' (paper presented at the 6th Annual International Conference on Information Warfare and Security, Washington, 17–18 March 2011) http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf. This discussion of the kill-chain concept is also informed by MITRE, Active Defense Strategy for Cyber (July 2012); and LTG Charles Croom, 'The Cyber Kill Chain: a Foundation for a New Cyber Security Strategy' (August 2020) 6 *High Frontier* 52–6, http://www.afspc.af.mil/shared/media/document/AFD-101019-079.pdf).

[131] In general, this also holds true for cyber activities with a hacktivist or criminal purpose.

military operations, these elements are not fully covered by military doctrine (yet). Without going into details, these rather 'novel' operations are therefore briefly described below.[132]

7. OPERATIONALISING MILITARY CYBER OPERATIONS

The military instrument of power will be used to achieve strategic objectives (of various kinds). Whether employed unilaterally or in a comprehensive manner together with other instruments of power, the military plans and executes operations to influence other actors. Obviously, these actors may be opposing forces, but more generically, these actors may also be friendly/supportive or neutral actors and audiences.[133] The military instrument, or, as referred to in doctrine, 'fighting power' comprises three components: conceptual, moral and physical (see Figure 13.4).



Source: © Haaster & Ducheine, 2014.

Figure 13.4 Fighting power in cyber operations

Through military operations, designed to achieve designated effects for strategic objectives, other actors are affected by alterations in their sources of power, either disruptively or constructively. Military operations – including cyber operations – will be directed 'against' the fighting power of another actor in order to achieve these effects.

---

[132] Using a model derived from: Paul AL Ducheine and Jelle van Haaster, 'Cyber-operaties en militair vermogen', 182 *Militaire Spectator* 368, 387; see also: Ducheine and Haaster, 'Fighting Power, Targeting and Cyber Operations' (n 6).

[133] For references, see Joint Doctrine Publications of various States, e.g., NL Ministerie van Defensie; US Department of Defense; and UK Ministry of Defence. For a detailed analysis: Ducheine and Haaster, 'Fighting Power, Targeting and Cyber Operations' (n 6).

The traditional addressees or 'targets' of these operations may be found in the physical (personnel, tangible objects, materiel and infrastructure) or in the virtual dimension. The latter comprises the psyche of personnel and information in general. By supporting actors with training, equipment or information, the physical, moral and conceptual component of their fighting power will increase, whereas attacking personnel, objects and manipulating information will decrease the (coherence between the) components of fighting power.

Cyber operations on the other hand, will make use of cyberspace comprising the physical network layer (i.e., the hardware) and two layers representing virtual elements: cyber identities and cyber objects.[134] First, the cyber persona layer contains cyber identities, i.e., the virtual reflection of persons, e.g., e-mail addresses, Facebook-accounts etcetera. Secondly, the logical network layer contains what could be called cyber objects (as a contrast to tangible objects in the physical dimension), e.g., applications (software or code) and data (stored or in process).

The uniqueness of cyber operations lies in the fact that the virtual dimension (as in Information Operations) offers new opportunities to influence actors. By addressing (or targeting) the cyber persona layer (i.e., cyber identities) and the logical network layer (i.e., cyber objects), disruptive and constructive effects can be achieved through cyber operations.

Conceptually, although thorny questions have been brought up and will remain to be addressed, the operational processes for physical or kinetic military operations and cyber operations are alike. This is also the case for the military process called 'targeting',[135] through which objectives are defined, potential targets selected, the available means are listed and evaluated in view of effectiveness and collateral consequences, the means are designated and prepared, and the action is executed and evaluated.[136]

Evidently, this brief conceptual description of military cyber operations offered is not unique for the military paradigm, as its operationalisation can be used in others as well by analogy. What remains exclusive, though, for military cyber operations executed by States, is the paradigm and the (legal) framework that is authorising and governing these activities. Unlike other paradigm, the (strategic) objectives defined are the most far reaching (or extreme) in its ends, means and effects.

8. CONCLUSION

This chapter set out to elaborate on the phenomenon of what is often coined as cyber operations as a common denominator for cyber activities. After having analysed differences in strategic or corporate objectives (for States and non-States alike), the similarities in terms of means to achieve those objects and the ways to employ those means on the operational level

---

[134] See n 6. On the status of cyberspace under international law see Tsagourias (Ch 1 of this Handbook).

[135] William H Boothby, *The Law of Targeting* (OUP 2012) 378 *ff*. In particular: Paul AL Ducheine and Terry D Gill, *From Cyber Operations to Effects: Some Targeting Issues*, *Militair Rechtelijk Tijdschrift* (2018) https://puc.overheid.nl/doc/PUC_248377_11/1/#d9bd4879-c519-4682-8570-4b541c0898e3.

[136] E.g., Robert Fanelli and Gregory Conti, 'A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict' in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *Proceedings of the 4th (2012) International Conference on Cyber Conflict* (CCD COE 2012) http://www.ccdcoe.org/publications/2012proceedings/5_5_Fanelli&Conti_AMethodologyForCyberOperationsTargeting.pdf.

(of States and non-State actors) were considered. Moreover, five distinct paradigms are used to shape cyber activities on the State level. The core paradigms – in particular law enforcement, intelligence and military operations – provide the legal basis for governmental powers that may interfere with human rights and privileges. Military operations within the paradigm of conflict represent the most far-reaching framework for governmental action.

Having said this, it is noteworthy that cyberspace and its actors are influenced by military jargon (at least). Notwithstanding the idiom used – think of attacks, targeting, cyber war – the majority of cyber activities are of a non-military nature. Once again, it appears that the main actors in cyberspace are intelligence agencies (governmental) or enterprises (corporate), and criminals (varying from individual to organised crime), and that their main objectives are sabotage, espionage, subversion[137] and crime.

[137] See National Cyber Security Centre, *Cyber Security Assessment Netherlands (CSAN)-3* and Rid (n 5).

14. Cyber operations as a use of force

Marco Roscini[1]

1. INTRODUCTION

Article 2(4) of the UN Charter famously provides that '[a]ll Members [of the United Nations] shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations'. This provision is generally considered to reflect customary international law and, at least with regard to its core, also *jus cogens*.[2] It is generally accepted that the fact that Article 2(4) was adopted well before the Information Age does not necessarily prevent its application to cyber operations.[3] States and international organizations that have affirmed the applicability of the existing rules on the use of force in the cyber context include

[1] This chapter is based on and updates considerations developed in the author's book *Cyber Operations and the Use of Force in International Law* (OUP 2014) 44–67, and takes into account events and law as of November 2019.

[2] The customary nature of art 2(4) has been recognized by the ICJ in *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US)* (Merits, Judgment) [1986] ICJ Rep 14, paras 187–90 [*Nicaragua Case*]. See also *Legal consequences of the construction of a wall in the occupied Palestinian territory* (Advisory Opinion) [2004] ICJ Rep 136, para 87. Several authors have argued that the core prohibition contained in art 2(4), that of aggression, is also a peremptory norm of general international law (Roberto Ago, Addendum to the Eighth Report on State Responsibility (1980) II/1 *Yearbook of the ILC* 44; Rein Müllerson, '*Jus ad bellum*: Plus Ça Change (Le Monde) Plus C'Est la Même Chose (Le Droit)?' (2002) 7 *J of Conflict and Security L* 149, 169; Natalino Ronzitti, *Diritto internazionale dei conflitti armati* (Giappichelli 2014) 33).

[3] The US Department of Defense defines 'cyberspace operations' as those which 'use cyber capabilities, such as computers, software tools, or networks' with the 'primary purpose of achieving objectives or effects in or through cyberspace' (US Department of Defense, Law of War Manual (June 2015 – Updated December 2016) 1012).

Australia,[4] Hungary,[5] China,[6] Cuba,[7] Estonia,[8] the European Union,[9] France,[10] Italy,[11] Mali,[12] the Netherlands,[13] Norway,[14] Qatar,[15] the Russian Federation,[16] the United Kingdom,[17] and the United States.[18] On the basis of the views submitted by UN member States, the 2013 Report of the Group of Governmental Experts set up by the UN General Assembly to examine threats in cyberspace also found that '[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [Information and Communications Technologies] environment'.[19] This conclusion was reaffirmed in the 2015 Report.[20]

---

[4] Australian Government, Australia's International Cyber Engagement Strategy (October 2017) Annex A, 90 https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT%20AICES_AccPDF.pdf accessed 30 November 2019.

[5] 'Welcome speech by János Martonyi, Minister of Foreign Affairs of Hungary' (Budapest Conference on Cyberspace, Opening Session, 4 October 2012) https://2010-2014.kormany.hu/en/ministry-of-foreign-affairs/speeches-publications-and-interviews/minister-of-foreign-affairs-janos-martony-s-speech-at-the-budapest-conference-on-cyberspace accessed 30 November 2019.

[6] Li Zhang, 'A Chinese perspective on cyber war' (2012) 94 *Intl Rev of the Red Cross* 801, 804.

[7] UN Doc A/57/166/Add.1, 29 August 2002, 3.

[8] President of the Republic's Speech at CyCon 2019, 29 May 2019, https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019 accessed 30 November 2019.

[9] *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (JOIN(2013) 1 final, 7 February 2013) 15–16 http://ec.europa.eu/information_society/newsroom/cf//document.cfm?doc_id=1667 accessed 30 November 2019. See also 'Speech by EU High Representative Catherine Ashton on Cyber security: an open, free and secure Internet' (SPEECH/12/685, Budapest, 4 October 2012) 3 http://europa.eu/rapid/press-release_SPEECH-12-685_en.htm accessed 30 November 2019.

[10] Ministère des Armées, *Droit international appliqué aux cyberopérations dans le cyberespace* (2019) 7 https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit%2Binternat%2Bappliqu%C3%A9%2Baux%2Bop%C3%A9rations%2BCyberespace.pdf accessed 30 November 2019.

[11] Governo Italiano, *La posizione italiana sui principi fondamentali di Internet* (17 September 2012) 5 http://download.repubblica.it/pdf/2012/tecnologia/internet.pdf accessed 30 November 2019.

[12] UN Doc A/64/129/Add.1, 9 September 2009, 7.

[13] Dutch Minister of Foreign Affairs, Letter to Parliament on the international legal order in cyberspace (5 July 2019) Appendix: International law in cyberspace 3–4 https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace accessed 30 November 2019.

[14] Norwegian Ministry of Defence, Manual of the Law of Armed Conflict, 2013, 209.

[15] UNGA 'Developments in the field of information and telecommunications in the context of international security' (20 July 2010) UN Doc A/65/154 9–10.

[16] Russian Federation, *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space* (unofficial translation by CCDCOE, 2011) 6 https://ccdcoe.org/uploads/2018/10/Russian_Federation_unofficial_translation.pdf accessed 30 November 2019.

[17] Cyber and International Law in the 21st Century, Speech by the Attorney General Jeremy Wright at Chatham House, 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century accessed 30 November 2019.

[18] US Department of Defense (n 3) 1015.

[19] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013) UN Doc A/68/98 8.

[20] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) UN Doc A/70/174 12–13.

For Article 2(4) and its customary counterpart to apply to cyber operations, however, three conditions must be met: (1) the cyber operation needs to be attributed to a State: conduct by private individuals or armed groups does not fall within the scope of the provision, not even when it results in damage comparable to that caused by States; (2) the cyber operation must amount to either a 'threat' or a 'use of force'; (3) the threat or use of force must be exercised in the conduct of 'international relations'. As to the first condition, the problems concerning the identification of the origin and the attribution of cyber operations to States are well-known and are probably the main obstacle to the application of Article 2(4) in the cyber context. They are however beyond the scope of this chapter, which will assume that a cyber operation has been attributed with sufficient certainty to a State.[21] The reference to 'international relations' in Article 2(4) entails that the cyber operations must not only be by a State, but also against another State: a State, therefore, is not prohibited by this provision to threaten or resort to cyber operations against non-State actors within its territory, not even when the operations amount to a threat or a use of force.[22] Finally, for Article 2(4) to apply, the cyber operation must qualify either as a threat or as a use of force. This chapter will focus only on the latter: as, in its 1996 Advisory Opinion on the *legality of the threat or use of nuclear weapons*, the International Court of Justice (ICJ) linked the legality of threats, be they explicit or implied in certain conduct, to the legality of the use of force in the same circumstances,[23] the considerations developed below in relation to cyber operations as a use of force also apply, *mutatis mutandis*, to those amounting to threats of the use of force.[24]

The determination of the threshold above which a cyber operation amounts to a use of force has proved to be a very contentious issue. The present chapter will address this problem and will first establish what is meant by 'armed' force and whether cyber operations can qualify as such. It will then distinguish between cyber attacks and cyber espionage and, within the former, between cyber attacks that cause, or are reasonably likely to cause, physical damage to persons or property, those that cause loss of functionality of infrastructures without physically damaging them, and other cyber attacks and cyber-related conduct. The overall purpose is to identify which of the above types of cyber activities qualify as a use of force and are therefore prohibited by Article 2(4) of the UN Charter.

2. CYBER OPERATIONS AS ARMED FORCE

As Article 2(4) of the UN Charter only prohibits the threat and the use of 'armed' force and not other forms of coercion,[25] the question is whether cyber operations can qualify as such. 'Armed force' is not identified on the basis of the authors of the forceful action, i.e., the armed

---

[21] On the identification and attribution problems, see Roscini (n 1) 33–40; Nicholas Tsagourias, 'Cyber attacks, self-defence and the problem of attribution' (2012) 17 *J of Conflict and Security L* 229, 233–43.

[22] The situation would be different if the non-State actors were located on and operated from the territory of another State.

[23] *Legality of the threat or use of nuclear weapons* (Advisory Opinion) [1996] ICJ Rep 226, para 47 [Nuclear weapons]. This conclusion was reaffirmed in the *Guyana and Suriname* Arbitral Award, 17 September 2007, 47 (2008) *International Legal Materials* 166, 229–30, para 439.

[24] Specifically on cyber operations and threats of force, see Roscini (n 1) 67–9.

[25] Ibid., 45–6.

forces, as otherwise States would easily avoid the application of the prohibition by outsourcing such actions to intelligence agencies or private contractors. In fact, incidents involving the armed forces but not the use of weaponry, like the violation of airspace or territorial waters by military aircraft or ships, are usually treated as violations of sovereignty, but not as a use of force under Article 2(4).[26] The presence of a coercive intention is also per se not sufficient to identify armed force. Indeed, 'armed force' is nothing other than an extreme form of intervention which, like economic and political coercion, is characterized by the intention of the coercing State to compel the victim State into doing or not doing something through a 'dictatorial interference' in its internal or external affairs.[27] Both the use of force and the broader notion of intervention, then, imply a coercive intention, and what differentiates the two must be found elsewhere.

Whether or not cyber operations fall within the scope of Article 2(4) depends ultimately on which of the three main analytic approaches to understanding the nature of a use of armed force is accepted. The instrument-based approach focuses on the means used to commit an act, i.e., weapons, and has been traditionally employed to distinguish armed force from economic and political coercion. This approach has been criticized for being centred on instruments defined by their physical characteristics: as such—it has been claimed—it is ill-suited to be extended to digital codes and would lead to the conclusion that cyber operations can never be a use of force under Article 2(4), even when they result in physical damage.[28] The target-based approach argues that cyber operations reach the threshold of the use of armed force when they are conducted against national critical infrastructure (NCI), whatever their effects on such infrastructure or the nature of the operation might be.[29] This approach, however, is over-inclusive in that it would also qualify as a use of force those cyber operations that only cause inconvenience or merely aim to collect information as long as they target a NCI. Another problem with this view—it has been argued—is that there is no generally accepted definition of 'NCI'.[30]

The approach that has received most support is based on the effects of the action: unlike other forms of coercion, armed force has direct destructive effects on property and persons.[31] Therefore, any cyber operation that causes, or is reasonably likely to cause, the damaging con-

---

[26] Oliver Dörr, 'Use of force, prohibition of' in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (OUP 2012) vol X, 607, 611.

[27] Hersch Lauterpacht, *International Law and Human Rights* (Stevens & Sons Ltd 1950) 167. On the principle of non-intervention, see section 3.C of this chapter.

[28] Stephanie Gosnell Handler, 'The new cyber face of battle: Developing a legal approach to accommodate emerging trends in warfare' (2012) 48 *Stanford J of Intl L* 209, 226–7; Matthew C Waxman, 'Self-defensive force against cyber attacks: Legal, strategic and political dimensions' (2013) 89 *Intl L Studies* 109, 111.

[29] Walter G Sharp, *Cyberspace and the Use of Force* (Aegis Research Corp 1999) 129–32. See similarly Christopher C Joyner and Catherine Lotrionte, 'Information warfare as international coercion: Elements of a legal framework' (2011) 12 *EJIL* 825, 855, who argue that stealing or compromising sensitive military information could also qualify as an armed attack (and *a fortiori* a use of force) 'even though no immediate loss of life or destruction results'.

[30] For a discussion of the different definitions of NCI, see Roscini (n 1) 55–8.

[31] See e.g., Russell Buchan, 'Cyber attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 *J of Conflict and Security L* 211, 212; Heather H Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012) 74.

sequences normally produced by kinetic weapons would be a use of armed force.[32] This view, however, does not take into account that the dependency of modern societies on computers, computer systems and networks has made it possible to incapacitate physical infrastructures without destroying them. Another problem with this approach is that directness is not necessarily an inherent characteristic of the use of armed force: the UN General Assembly's Declaration on the Definition of Aggression, for instance, qualifies as an 'act of aggression', i.e., 'the most serious and dangerous form of the illegal use of force',[33] not only bombings and invasions, but also actions which do not necessarily entail direct destructive effects, such as the violation of a stationing agreement, a naval blockade, and allowing the use of the territory by other States for the purpose of perpetrating aggression.[34] In the *Nicaragua* judgment, the ICJ also qualified the arming and training of armed groups—not directly destructive actions—as a use of force.[35]

It is submitted, therefore, that it is preferable to identify 'armed' force by reference to the instruments used. This is consistent with the ordinary meaning of the expression:[36] according to *Black's Law Dictionary*, 'armed' means '[e]quipped with a weapon' or '[i]nvolving the use of a weapon'.[37] Unlike mere intervention, armed force entails the cumulative presence of two elements: the use of weapons and an intention to coerce.[38] As a consequence, a limited use of weapons by a State that is not directed at exercising coercion on another State, as in the case of police measures at sea, interception of trespassing aircraft or international abductions, does not fall under the scope of Article 2(4), but may be a violation of other norms, such as the duty to respect another State's territorial sovereignty.[39] Similarly, economic measures that cause starvation among the population are not a use of armed force in spite of their severe humanitarian consequences and of their coercive intention, because they do not entail the use of weapons: economic measures may be enforced with the use of weapons, but are not weapons themselves, as implied in Article 41 of the UN Charter.[40]

---

[32] Dinstein has, for instance, argued that 'what counts is not the specific type of ordnance, but the end product of its delivery to a selected objective' (Yoram Dinstein, 'Computer network attacks and self-defense' (2002) 76 *Intl L Studies* 99, 103). Silver also opines that 'physical injury or property damage must arise as a direct and foreseeable consequence of the CNA [Computer Network Attack] and must resemble the injury or damage associated with what, at the time, are generally recognized as military weapons' (Daniel B Silver, 'Computer network attack as a use of force under Article 2(4) of the United Nations Charter' (2002) 76 *Intl L Studies* 73, 92–3).

[33] Definition of Aggression, GA Res 3314 (XXIX) 14 December 1974, Preamble.

[34] Ibid., art 3(c), (e), and (f).

[35] *Nicaragua Case* (n 2) para 228.

[36] According to art 31(1) of the 1969 Vienna Convention on the Law of Treaties, '[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose' (UNTS, vol 1115, 331 *ff*).

[37] Bryan A Garner (ed), *Black's Law Dictionary* (Thomson-West 2009) 123.

[38] As has been observed,

> [t]he essential feature which characterizes the prohibition of the use of force is . . . not the intrusion into the sovereign realm of another State, nor is it even the element of coercion as such, but only an intrusion or coercion accompanied by the special features of military weaponry and its actual use

(Dörr (n 26) 611).

[39] See Olivier Corten, *The Law Against War. The Prohibition on the Use of Force in Contemporary International Law* (Hart 2010) 66–7.

[40] Art 41 of the UN Charter includes the 'complete or partial interruption of economic relations' in the list of 'measures not involving the use of armed force'.

Although there is no binding definition of 'weapon' either in *jus ad bellum* or *jus in bello* instruments, *Black's Law Dictionary* defines it as '[a]n instrument used or designed to be used to injure or kill someone'.[41] The ICRC Study on *Customary International Humanitarian Law* defines weapons as 'means to commit acts of violence against human or material enemy forces'.[42] Rule 1(ff) of the *HPCR Manual on International Law Applicable to Air and Missile Warfare* (the 'HPCR Manual') also attaches one main characteristic to a weapon: the capability to cause either injury/death of persons or damage/destruction of objects.[43] Similarly, a leading commentator has defined weapons as including 'any arms … munitions … and other devices, components or mechanisms striving to (i) kill, disable or injure enemy personnel; or (ii) destroy or damage *matériel* or property'.[44] The minimum common denominator of the above definitions is the violent consequences produced by the instrument. Weapons, therefore, are identified by their effects, not by the mechanisms through which they produce destruction or damage.[45] If this is correct, armed force prohibited by Article 2(4) could be defined as the form of intervention by a State to exercise coercion on another State that involves the use of instruments (weapons) capable of producing violent consequences. At a closer look, then, the debate between the supporters of the instrument-based and effects-based approaches to establish whether cyber operations are a use of armed force loses much of its significance, as the two approaches should be combined: it is the instrument used that defines armed force, but the instrument is identified by its (violent) consequences. The focus on instrumentality explains why the ICJ qualified arming and training of armed groups as a use of force:[46] although not directly destructive, those activities are strictly related to weapons, as they aim at enabling someone to use them.

If, then, a use of armed force under Article 2(4) requires weapons, the next step in the analysis is to establish whether malware can qualify as such. In its Advisory Opinion on the *Legality of the threat or use of nuclear weapons*, the ICJ made clear that Articles 2(4), 51 and 42 of the UN Charter 'do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed'.[47] There is then no reason why the weapons covered by these provisions should necessarily have explosive effects or be created for offensive purposes only: the use by a State of certain dual-use non-kinetic weapons, such as biological or chemical agents, against another State would undoubtedly be treated by the latter as a use of force in the sense of Article 2(4). According to Brownlie, this is so because chemical and biological weapons are commonly referred to as forms of 'warfare' and because they can be used to destroy life and property:[48] both arguments would suit at least some malware as well. In particular, several States have included cyber technologies in their military doctrines, refer to cyberspace as to

---

41 Garner (n 37) 1730.

42 Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law* (CUP 2005) vol I, rule 6.

43 Program on Humanitarian Policy and Conflict Research [HPCR], *Manual on International Law Applicable to Air and Missile Warfare* (CUP 2013) 49.

44 Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (CUP 2016) 2.

45 Katharina Ziolkowski, 'Computer network operations and the law of armed conflict' (2010) 49 *Military Law and Law of War Review* 47, 69.

46 *Nicaragua Case* (n 2) para 228.

47 *Nuclear weapons* (n 23) para 39.

48 Ian Brownlie, *International Law and the Use of Force by States* (Clarendon Press 1963) 362.

a fifth domain of warfare and have set up military units with specific cyber expertise.[49] The Russian Foreign Minister warned that the destructive effects of information weapons 'may be comparable to that of weapons of mass destruction'.[50] Belarus made the same analogy.[51] Kazakhstan observed that 'information technology advances may be misused as information weapons during armed conflicts'.[52] Cuba also remarked that '[i]nformation and telecommunication systems can be turned into weapons when they are designed and/or used to damage the infrastructure of a State, and as a result, can put at risk international peace and security'.[53] Spain recalled the '[u]se of the Internet as a weapon, i.e., its use as a means to launch attacks against critical infrastructure information systems or the infrastructure of the Internet itself'.[54] The French Ministry of Defence's 2019 document also refers to 'cyber-armes' which can have effects that are material or immaterial, temporary, reversible or non-reversible.[55] The US Law of War Manual provides that at least certain cyber capabilities constitute weapons or weapons system and their acquisition must therefore be reviewed.[56] The 2010 UK National Security Strategy emphasizes that 'activity in cyberspace' is 'a military weapon for use by states and possibly others'.[57] Finally, the International Committee of the Red Cross has stated that the obligation provided in Article 36 of the 1977 Protocol I Additional to the 1949 Geneva Conventions on the Protection of Victims of War applies to cyber capabilities that qualify as weapons, means and methods of warfare.[58]

All the above supports the view that 'cyber … must be looked upon as a new means of warfare—in other words, a weapon: no less and no more than other weapons'.[59] The Commentary to the *HPCR Manual* confirms that '[m]eans of warfare include non-kinetic systems, such as those used in EW [electronic warfare] and CNAs [Computer Network Attacks]. The means would include the computer and computer code used to execute the

---

[49] See the examples mentioned in Roscini (n 1) 3–4, 9–10.

[50] Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, UN Doc A/C.1/53/3, 30 September 1998, 2.

[51] UN Doc A/54/213, 10 August 1999, 3.

[52] UN Doc A/64/129, 8 July 2009, 5.

[53] UN Doc A/66/152/Add.1, 16 September 2011, 2.

[54] UN Doc A/64/129/Add. 1 (n 12) 10.

[55] Ministère des Armées (n 10) 13.

[56] Department of Defense (n 3) 1025–26.

[57] Prime Minister, 'A Strong Britain in an Age of Uncertainty: The National Security Strategy' (Cm 7953, 2010) 29 https://www.gov.uk/government/publications/the-national-security-strategy-a-strong-britain-in-an-age-of-uncertainty accessed 30 November 2019.

[58] International Committee of the Red Cross, International Humanitarian Law and Cyber Operations during Armed Conflict, Position paper (November 2019) https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts accessed 30 November 2019. Art 36 of Additional Protocol I provides that '[i]n the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party' (text in UNTS, vol 1125, 3 *ff*).

[59] Yoram Dinstein, 'Cyber war and international law: Concluding remarks at the 2012 Naval War College International Law Conference' (2013) 89 *International Law Studies* 276, 280. Schmitt also notes that '[w]ith the advent of CNA, today the computer is no less a weapon than an F-16 armed with precision weapons' (Michael N Schmitt, 'Computer network attack: The normative software' (2001) 4 *Ybk of Intl Humanitarian L* 53, 56).

attack, together with all associated equipment'.[60] The Commentary further specifies that death, injury, damage, or destruction 'need not result from physical impact … since the force used does not need to be kinetic. In particular, CNA hardware, software and codes are weapons that can cause such effects through transmission of data streams'.[61] Like missiles, cyber weapons include a delivery system, a navigation system and a payload.[62] The delivery system could go from e-mails to malicious links in websites, hacking, counterfeit hardware and software. System vulnerabilities are the main navigation systems that provide entry points for the payload by enabling unauthorized access to the system. The payload is the component that causes harm: if the code, however sophisticated, is designed solely for the purpose of infiltrating a computer and exfiltrating information, it would not be a 'weapon' in the sense highlighted above, as it is neither intended to nor capable of causing violent consequences.[63]

3. THE APPLICATION OF ARTICLE 2(4) OF THE UN CHARTER TO DIFFERENT TYPES OF CYBER OPERATIONS

When a cyber operation conducted by a State against another employs a weapon and is accompanied by a coercive intent, then, it potentially amounts to a use of armed force under Article 2(4) of the UN Charter. As already noted, however, not all cyber operations entail the use of a 'weapon', which distinguishes cyber espionage from cyber attacks. Cyber espionage (or, as is referred to in US documents, cyber 'exploitation') constitutes unauthorized access to computers, computer systems or networks, in order to collect information, but without affecting the functionality of the accessed system or corrupting, amending or deleting the data resident therein. As has been observed, '[t]he primary technical difference between cyber attack and cyberexploitation is in the nature of the payload to be executed—a cyber attack payload is destructive whereas a cyberexploitation payload acquires information nondestructively'.[64] Although they are often labelled in the press as 'cyber attacks', cyber espionage operations are different as they focus on intelligence collection, surveillance and reconnaissance rather than on system disruption and may be preliminary to a cyber attack (whether amounting to a use of force or not) that they aim to enable, for instance by mapping the architecture of the target network or operating system or by identifying previously unknown vulnerabilities. Stealing security data or intellectual property from governments and corporations may also be an aim in itself and is a major threat to national security and commerce.[65]

---

[60] HPCR Manual (n 42) 31.

[61] Ibid., 49.

[62] Fred Schreier, 'On cyberwarfare' (DCAF Horizon 2015 Working Paper no 7, 2012) 66–67 https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf accessed 30 November 2019.

[63] Thomas Rid and Peter McBurney, 'Cyber-weapons' (2012) 157 *RUSI J* 6, 11.

[64] Herbert S Lin, 'Offensive cyber operations and the use of force' (2010) 4 *J of National Security L and Policy* 63, 64. On cyber espionage, see Russell Buchan, *Cyber Espionage and International Law* (Hart 2018) and Buchan and Navarrete (Ch 11 of this Handbook).

[65] As has been noted, 'the cyber context changes the scale and consequences of theft and espionage to a degree that can result in harm to the country at least as severe as a physical attack' (Jack Goldsmith, 'How cyber changes the laws of war' (2013) 24 *EJIL* 129, 133).

Cyber espionage may violate the sovereignty of a State when it entails an unauthorized intrusion into cyber infrastructure located on its territory,[66] but can never ontologically amount to a use of armed force in the sense of Article 2(4) of the UN Charter, as it does not involve the use of weapons, i.e., cyber capabilities with a payload designed to produce violent consequences.[67] In contrast, cyber attacks are those cyber operations, whether in offence or in defence, aimed at altering, deleting, corrupting or denying access to computer data or software for the purposes of: (a) propaganda or deception; and/or (b) partly or totally disrupting the functioning of the targeted computer, computer system or network, and related computer-operated physical infrastructure (if any); and/or (c) producing physical damage extrinsic to the computer, computer system or network. A cyber attack can therefore go from relatively innocuous psychological operations, such as website defacement, to acts that cause havoc in military campaigns by generating misinformation, or acts resulting in major disruption of services and loss of property and lives. A 'cyber attack' could be a use of force under Article 2(4) of the UN Charter, an 'armed attack' in the sense of Article 51 for self-defence purposes,[68] or an 'attack' under Article 49(1) of Protocol I Additional to the 1949 Geneva Conventions on the Protection of Victims of War, but care should be taken not to see these expressions as coterminous.[69] In particular, cyber attacks can potentially fall under the scope of the prohibition contained in Article 2(4) when they entail the use of cyber tools capable of producing certain damaging consequences. The different sets of consequences deriving from a cyber attack will be examined in the following sub-sections in order to determine when they amount to a use of force.

(a) Cyber Attacks Causing, or Reasonably Likely to Cause, Physical Damage to Property, Loss of Life, or Injury of Persons

There is general agreement that, if a cyber attack employs capabilities that cause, or are reasonably likely to cause, physical damage to property, loss of life or injury of persons in a manner equivalent to kinetic attacks through the alteration, deletion or corruption of software or data, it will fall under the prohibition contained in Article 2(4) of the UN Charter. According to the US Law of War Manual, for instance, 'if cyber operations cause effects that, if caused by traditional physical means, would be regarded as a use of force under *jus ad bellum*, then such cyber operations would likely also be regarded as a use of force'.[70] The Manual cites, as examples of cyber operations amounting to a use of force, operations that trigger a nuclear

---

[66] Buchan (n 64) 49–55; Wolff Heintschel von Heinegg, 'Territorial sovereignty and neutrality in cyberspace' (2013) 89 *Intl L Studies* 123, 129.

[67] For a critique of views that qualify 'cyber espionage' as a use of force, see Buchan (n 64) 65–8; Katharina Ziolkowski, 'Peacetime cyber espionage – New tendencies in public international law' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (CCDCOE 2013) 425, 451–7.

[68] On cyberattacks and self-defence see Focarelli (Ch 15 of this Handbook).

[69] On cyber attacks as 'armed attack' under art 51 of the UN Charter and as 'attack' under the law of armed conflict see Roscini (n 1) 70–7, 178–82.

[70] US Department of Defense (n 3) 1015. See also Rule 69 of the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) 330. The *Manual*, that aims to identify how the *lex lata* applies to cyber operations, was prepared by a group of experts at the invitation of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) but does not reflect NATO doctrine or the official position of any State or organization.

plant meltdown, operations that open a dam in a populated area leading to destructive flooding, and operations that disable air traffic control causing planes to crash.[71] For France, '*[u]ne cyber-opération conduite par un État à l'encontre d'un autre Etat constitue une violation du principe d'interdiction de recourir à la force si ses effets sont similaires à ceux qui résultent de l'utilisation d'armes classiques*'.[72] The same position has been adopted by the Netherlands.[73] Australia's 2017 Cyber Engagement Strategy also affirms that:

> [i]n determining whether a cyber attack, or any other cyber activity, constitutes a use of force, states should consider whether the activity's scale and effects are comparable to traditional kinetic operations that rise to the level of use of force under international law [which] involves a consideration of the intended or reasonably expected direct and indirect consequences of the cyber attack, including for example whether the cyber activity could reasonably be expected to cause serious or extensive ('scale') damage or destruction ('effects') to life, or injury or death to persons, or result in damage to the victim state's objects, critical infrastructure and/or functioning.[74]

It should be incidentally noted that physical damage to property, loss of life and injury of persons are only secondary or tertiary effects of a cyber attack resulting from the corruption, alteration or deletion of data or software.[75] This is, however, not necessarily a problem for the application of the *jus ad bellum* rules: in the *Nicaragua* judgment, the ICJ expressly recognized that intervention that uses armed force may occur either directly or indirectly.[76]

No cyber attack has so far been reported to have caused injuries or deaths of persons. If one excludes the almost legendary case of the explosion of a Soviet gas pipeline in Siberia in June 1982, apparently caused by a logic bomb inserted in the computer-control system by the Central Intelligence Agency (CIA),[77] the first known use of malicious software designed to produce material damage by attacking the Supervisory Control and Data Acquisition (SCADA) system of a NCI is Stuxnet. Using four unknown vulnerabilities, Stuxnet was allegedly designed to force a change in the gas centrifuges' rotor speed at the Natanz uranium enrichment plant in Iran, inducing excessive vibrations or distortions that would eventually damage the centrifuges.[78] As a result, the International Atomic Energy Agency (IAEA)

---

71 US Department of Defense (n 3) 1015.

72 Ministère des Armées (n 10) 7.

73 Dutch Minister of Foreign Affairs (n 13) 3–4.

74 Australian Goverment (n 4) 90.

75 The primary effects are those on the attacked computer, computer system or network, i.e., the deletion, corruption, or alteration of data or software, or system disruption through a Distributed Denial of Service (DDoS) attack or other cyber attacks. As Waxman notes, 'modern society's heavy reliance on interconnected information systems means that the indirect and secondary effects of cyber-attacks may be much more consequential than the direct and immediate ones' (Matthew C Waxman, 'Cyber attacks and the use of force: Back to the future of Article 2(4)' (2011) 36 *Yale J of Intl L* 421, 445). On the multiple effects of cyber attacks, see William A Owens, Kenneth W Dam, and Herbert S Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (The National Academies Press 2009) 80. See also Pia Palojärvi, *A Battle in Bits and Bytes: Computer Network Attacks and the Law of Armed Conflict* (Erik Castrén Institute of International Law 2009) 32; William H Boothby, 'Methods and means of cyber warfare' (2013) 89 *Intl L Studies* 387, 390.

76 *Nicaragua Case* (n 1) para 205.

77 Thomas Rid, *Cyber War Will Not Take Place* (Hurst & Co 2013) 4.

78 David Albright, Paul Brannan and Christina Walrond, 'Did Stuxnet take out 1,000 centrifuges at the Natanz Enrichment Plant?' (ISIS Report, 22 December 2010) 6 http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf accessed 30 November 2019.

reported that Iran stopped feeding uranium into thousands of centrifuges at Natanz, a claim denied by the Iranian authorities.[79]

One could ask whether there is a minimum threshold of gravity that the destructive consequences of a cyber attack need to reach in order to be a violation of Article 2(4) and not only of the principle of non-intervention. The former US Department of State's Legal Advisor, Harold Koh, for instance, appears to distinguish between injury/death of persons on the one hand and damage to property on the other when he argues that it is '[c]yber activities that proximately result in death, injury or *significant* destruction' that would be considered a use of force:[80] in his view, then, while any death or injury would turn a cyber operation into a use of force, only destruction that is significant enough would qualify. Beyond the cyber context, Corten maintains that 'there is a threshold below which the use of force in international relations, while it may be contrary to certain rules of international law, cannot violate article 2(4)':[81] examples are international abductions, extraterritorial enforcement measures, international police operations, hot pursuit and police measures at sea, and the interception and neutralization of aircraft entering a State's airspace without authorization. Similarly, in its 2009 Report, the Independent International Fact-Finding Commission on the Conflict in Georgia found that '[t]he prohibition of the use of force covers all physical force which surpasses a minimum threshold of intensity' and that '[o]nly very small incidents lie below this threshold, for instance the targeted killing of single individuals, forcible abductions of individual persons, or the interception of a single aircraft'.[82] There seems to be some cautious support for this view in the 1998 ICJ's *Fisheries Jurisdiction* Judgment: while Spain argued that the forcible measures against the *Estai* amounted to a violation of Article 2(4), the Court found that 'the use of force authorized by the Canadian legislation and regulations falls within the ambit of what is commonly understood as enforcement of conservation and management measures' and that '[b]oarding, inspection, arrest and *minimum* use of force for those purposes are all contained within the concept of enforcement of conservation and management measures according to a "natural and reasonable" interpretation of this concept'.[83]

There is nothing, however, in the wording of Article 2(4) suggesting that uses of force should be distinguished according to their gravity: as Ago notes, Article 2(4) prohibits 'any kind of conduct involving any assault whatsoever on the territorial sovereignty of another

---

[79] William J Broad, 'Report suggests problems with Iran's nuclear effort', *The New York Times* (23 November 2010) www.nytimes.com/2010/11/24/world/middleeast/24nuke.html accessed 30 November 2019. On the legality of Stuxnet and other cyber operations against Iran, see Marco Roscini, 'Cyber operations as nuclear counterproliferation measures' (2014) 19 *J of Conflict and Security L* 133.

[80] Harold Koh, 'International law in cyberspace' (Speech at the USCYBERCOM Inter-Agency Legal Conference, 18 September 2012) in CarrieLyn D Guymon (ed), *Digest of United States Practice in International Law* (United States Department of State 2012) 593, 595 (emphasis added). It should, however, be recalled that, according to the US position as reflected in Koh's speech, there is no distinction between 'use of force' and 'armed attack'.

[81] Corten (n 39) 55.

[82] Independent Fact-Finding Mission on the Conflict in Georgia, 'Report of the Independent Fact-Finding Mission on the Conflict in Georgia' (vol II, September 2009) 242 https://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf accessed 30 November 2019.

[83] *Fisheries Jurisdiction (Spain v Canada)* (Judgment) [1998] ICJ Rep 432, para 84 (emphasis added). See similarly the Report of the Commission of Inquiry (Denmark–United Kingdom) on the *Red Crusader* incident, 23 March 1962 [1967] 35 *International Law Reports* 485 *ff*.

State, irrespective of its magnitude, duration or purposes'.[84] Whether or not a 'minimum use of force' is a violation of Article 2(4) must ultimately depend on the circumstances of each case: what can be said is that the more invasive and damaging the use of (cyber) weapons, the more the affected State will be inclined to treat it as a use of force.

Whether data can be equated to physical property for the purposes of Article 2(4), so that their deletion, alteration or corruption qualify per se as a use of force even when they do not also result in physical damage to property, loss of life, bodily injury, or malfunction of infrastructures, is a hotly debated question. In August 2012, for instance, a virus destroyed the data of about 30,000 company computers of Saudi Aramco, the world's largest oil producer. The deleted data were replaced with a burning American flag.[85] John Murphy notes that '[i]f one views data as a form of property, indeed a very important form of property, in the modern world, a mass loss of data could constitute an armed attack' (and therefore, *a fortiori*, a use of force).[86] There is no indication, however, that States are willing to interpret Article 2(4) so broadly: as a commentator has argued, the mere destruction of data, even when of considerable importance, is not a use of force, as its 'effects cannot be equated to the effects usually caused or intended by conventional or BC [biological and chemical] weapons, especially not to the physical destruction of the objects'.[87] If not of Article 2(4), cyber attacks deleting, modifying or corrupting data without consequences in the analogue world may however be a violation of the principle of non-intervention, as will be seen later.[88]

(b) Cyber Attacks Causing Mere Loss of Functionality of Infrastructures

If cyber attacks employing capabilities that cause or are reasonably likely to cause material damage to property or persons can be equated to kinetic attacks, there is disagreement on whether cyber operations aimed at rendering ineffective or unusable infrastructures without physically damaging them[89] also amount to a violation of Article 2(4) of the UN Charter.

The present author has argued since 2010 that cyber operations causing mere loss of functionality of infrastructures could also be considered as falling under the prohibitive scope of Article 2(4) if the loss of functionality is significant enough to affect State security, or, to use the words of the 2012 US Presidential Policy Directive 20, 'national security, public safety, national economic security, the safe and reliable functioning of "critical infrastructure,"

---

[84] Ago (n 2) 41. Similarly, Melzer argues that art 2(4) prohibits all uses of force, regardless of their magnitude and duration (Nils Melzer, *Cyberwarfare and International Law* (UNIDIR 2011) 8 https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf accessed 30 November 2019).

[85] 'Saudi Aramco says cyber attack targeted kingdom's economy', *Al Arabiya News* (9 December 2012) www.alarabiya.net/articles/2012/12/09/254162.html accessed 30 November 2019. Oil production, however, remained uninterrupted.

[86] John F Murphy, 'Cyber war and international law: Does the international legal process constitute a threat to U.S. vital interests?' (2013) 89 *Intl L Studies* 309, 325.

[87] Katharina Ziolkowski, 'General principles of international law as applicable in cyberspace' in Ziolkowski (n 67) 135, 174.

[88] See below, sec 3(c).

[89] The language is borrowed from the definition of 'neutralize' contained in US Department of Defense, *Dictionary of Military and Associated Terms* (As of November 2019) 153 https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf accessed 30 November 2019.

and the availability of "key resources"'.[90] This is certainly the case of cyber operations that severely disrupt defence-related NCIs.[91] The 1999 US Department of Defense's *Assessment of International Legal Issues in Information Operations*, for instance, argues that 'corrupting the data in a nation's computerized systems for managing its military fuel, spare parts, transportation, troop mobilization, or medical supplies', therefore seriously interfering 'with its ability to conduct military operations', might be treated as a use of force.[92] The more recent 2015 US Law of War Manual[93] and the 2019 French Ministère des Armées' document on the application of international law in cyberspace[94] adopt the same view. If a cyber operation seriously disrupting defence functions is considered a use of force, this conclusion must also be correct for a cyber operation that aims at taking control of networked weapons and weapon systems of another State, such as missiles, satellites and drones. A possible example would be the cyber attack allegedly conducted in 2019 by the United States against the weapons systems used by Iran's Islamic Revolutionary Guard Corps, which had shot down a US drone and which the US argues also attacked oil tankers in the Persian Gulf.[95] It has been reported that the systems were disabled for a period of time.

Cyber attacks causing significant loss of functionality of other NCIs such as emergency and rescue services, energy, public health, transportation, food and water supply will in most cases also result, or will be likely to result, in some physical damage to property or persons. In particular, prolonged electricity shortage due to a cyber attack disrupting the national grid is likely to have severe negative repercussions on other NCIs and on virtually all sectors of society.[96] But even when no physical consequences arise, as in the case of cyber attacks against the banking and finance, government and communications sectors, 'a flexible interpretation [of Article 2(4)] according to the evolution of weaponry and the logic behind this provision does not prevent a broadening of its prohibition in order to incorporate new uses of force'.[97] The concept of dynamic, or evolutionary, interpretation, which is also implied in Article 31(3)(b) of the Vienna Convention on the Law of Treaties,[98] has been employed by the ICJ on several

---

[90] 'US Presidential Policy Directive/PPD–20' (October 2012) 3 https://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas accessed 30 November 2019.

[91] Katharina Ziolkowski, 'Computer network operations and the law of armed conflict' (2010) 49 *Military Law and Law of War Review* 47, 73–4; Tsagourias (n 21) 232.

[92] US Department of Defense 'An Assessment of International Legal Issues in Information Operations' (May 1999) 18 https://fas.org/irp/eprint/io-legal.pdf accessed 30 November 2019.

[93] US Law of War Manual (n 3) 1015–6.

[94] Ministère des Armées (n 10) 7.

[95] 'US "launched cyber-attack on Iran weapons systems"', *BBC News*, 23 June 2019 https://www.bbc.co.uk/news/world-us-canada-48735097 accessed 30 November 2019.

[96] Although it was not the consequence of a cyber attack, for instance, in June 2019 a massive power cut left millions without electricity in South America, with negative repercussions on the transport and water distribution systems (Tom Phillips and Uki Goñi, 'Millions across South America hit by massive power cut', *The Guardian* (16 June 2019) https://www.theguardian.com/world/2019/jun/16/millions-across-south-america-hit-by-massive-power-cut-argentina-uruguay-paraguay-brazil accessed 30 November 2019).

[97] Antonio Segura-Serrano, 'Internet regulation and the role of international law' (2006) 10 *Max Planck Ybk of UN L* 191, 224–5.

[98] According to art 31(3)(b) of the Vienna Convention, treaties shall be interpreted taking into account, inter alia, 'any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation'. Such practice includes 'documents, arrangements, and actions that express a specific understanding of the treaty' (Matthias Herdegen, 'Interpretation in

occasions. In the Judgment on the *Dispute Regarding Navigational and Related Rights (Costa Rica v Nicaragua)*, for instance, the ICJ found that 'where the parties have used generic terms in a treaty … [they] must be presumed, as a general rule, to have intended those terms to have an evolving meaning'.[99] The Court gave the example of 'commerce',[100] but the same reasoning could be applied to 'force'. From this perspective, it is interesting that Panama noted that misuse of information and telecommunication systems is a 'new form of violence', thus highlighting that violent effects are not limited to physical damage.[101] The increasing dependency of States on computer systems and networks to provide critical services for the society as well as the increasing severity and sophistication of cyber attacks should thus be taken into account when interpreting Article 2(4). As a report suggests, focusing only on destructive consequences on individuals and property is reductive in the cyber context, as 'modern society depends on the existence and proper functioning of an extensive infrastructure that itself is increasingly controlled by information technology': therefore, '[a]ctions that significantly interfere with the functionality of that infrastructure can reasonably be regarded as uses of force, whether or not they cause immediate physical damage'.[102] Melzer concurs and notes how the kinetic equivalence doctrine, that considers as a use of force only those cyber operations that cause material damage comparable to kinetic weapons, is too restrictive.[103] Similarly, Tsagourias emphasizes that 'a cyber attack on critical State infrastructure which paralyses or massively disrupts the apparatus of the State should be equated to an armed attack, even if it does not cause any immediate human injury or material damage'.[104] Indeed, the limits of the doctrine of kinetic equivalence become evident if one considers that, under this doctrine, a cyber attack that shuts down the national grid or the stock exchange for a prolonged time would not be a use of armed force, while the physical destruction of one server in theory would.

An 'interpretive reorientation'[105] of Article 2(4) that also includes in the scope of the provision cyber attacks causing serious disruption of essential services without destroying infrastructures would also reflect the trend in modern warfare to favour incapacitation to destruction. In the 1999 Operation Allied Force against Yugoslavia, for instance, NATO targeted switching stations instead of generation stations to enable fast repair after the conflict

---

international law' in Wolfrum (ed), *Max Planck Encyclopedia* (n 25) vol VI, 260, 263). See also Rudolf Bernhardt, 'Evolutive treaty interpretation, especially of the European Convention on Human Rights' *German Yearbook of Intl L* 42 (1999) 11, 15.

[99] *Dispute Regarding Navigational and Related Rights (Costa Rica v Nicaragua)* (Judgment) [2009] ICJ Rep 213, para 66. See also *Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970)* (Advisory Opinion) [1971] ICJ Rep 16, para 53, where the Court found that 'an international instrument has to be interpreted and applied within the framework of the entire legal system prevailing at the time of the interpretation'.

[100] *Dispute Regarding Navigational and Related Rights*, ibid., para 70.

[101] UN Doc A/57/166/Add.1, 29 August 2002, 5.

[102] Owens, Dam and Lin (n 75) 254. Similarly, Brown and Poellet argue that '[a]lthough no actual kinetic event may occur, the reliance of modern societies on electricity for health care, communications, and the delivery of essential services makes it clear this would qualify as a kinetic-like effect and would therefore constitute a military attack if the disruption were for a significant period of time' (Gary Brown and Keira Poellet, 'The customary international law of cyberspace' (2012) 6 *Strategic Studies Quarterly* 126, 137).

[103] Melzer (n 84) 14.

[104] Tsagourias (n 21) 231.

[105] Waxman (n 75) 437.

and used carbon-graphite filaments in such a way as to cause only temporary incapacitation of electricity.[106] The Rules of Engagement distributed to the US Military Forces in Operation Iraqi Freedom also provided that attacks on the enemy infrastructure, lines of communication and economic objects should be aimed at disabling and disrupting them, avoiding destruction whenever possible.[107] Like non-lethal weapons, cyber operations should be understood in this context.[108]

Although it is not the only decisive factor as the supporters of the target-based approach suggest, the critical character of the targeted infrastructure is an important element to establish when a cyber operation causing mere loss of functionality amounts to a use of force under Article 2(4), in particular as an indication of the severity of its effects on a State.[109] It is especially helpful to *exclude* that the operation is a use of force: if the targeted infrastructure is *not* a NCI, it is highly unlikely that the resulting disruption will affect a State's essential functions and its internal public order. A cyber attack on a NCI, however, is not necessarily always a use of force, for instance when it disables it only for a very limited time or with limited effects.

Several States have expressed the view that cyber operations causing loss of functionality of certain infrastructures, in particular those related to the economy, can constitute a use of force. Mali, for instance, has claimed that:

> [t]he use of an information weapon could be interpreted as an act of aggression if the victim State has reasons to believe that the attack was carried out by the armed forces of another State and was aimed at disrupting ….economic capacity, or violating the State's sovereignty over a particular territory.[110]

The US Department of Defense's *Assessment of International Legal Issues in Information Operations* refers to a nation's air traffic control system, its banking and financial system, and public utilities and dams as examples of targets that, if shut down by a coordinated computer network attack, might entitle the victim State to self-defence.[111] The 2011 Department of Defense's *Cyberspace Policy Report* maintains that the US reserves the right to use 'all necessary means' against 'hostile acts', including 'significant cyber attacks', directed not only against the US Government or military but also the economy.[112] In 2018, the Dutch Minister of Defence, quoting an earlier report, affirmed that if 'a cyber-attack targets the entire Dutch financial system … or if it prevents the government from carrying out essential tasks such

---

[106] Dominik Steiger, 'Civilian objects' in Wolfrum (ed), *Max Planck Encyclopedia* (n 26) vol II, 185, 187.

[107] Human Rights Watch, 'Off target. The conduct of the war and civilian casualties in Iraq' (2003) 138–9, www.hrw.org/reports/2003/usa1203/usa1203.pdf accessed 30 November 2019.

[108] NATO has defined non-lethal weapons as 'weapons which are explicitly designed and developed to incapacitate or repel personnel, with a low probability of fatality or permanent injury, or to disable equipment, with minimal undesired damage or impact on the environment' ('NATO Policy on Non-Lethal Weapons' (Press Statement, 13 October 1999) www.nato.int/docu/pr/1999/p991013e.htm accessed 30 November 2019).

[109] This seems suggested in the document delineating France's view on the application of international law in cyberspace (Ministère des Armées (n 10) 7).

[110] UN Doc A/64/129/Add. 1 (n 12) 8.

[111] US Department of Defense (n 92) 18.

[112] US Department of Defense, 'Cyberspace Policy Report. A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934' (November 2011) 4 https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf accessed 30 November 2019.

as policing or taxation … it would qualify as an armed attack' (and, *a fortiori*, to a use of armed force),[113] and, in a July 2019 letter to parliament, the Dutch Minister of Foreign Affairs maintained that 'it cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as the use of force'.[114] France's official position is also that certain cyber operations could breach the prohibition of the use of force even in the absence of physical effects, particularly when it causes '*des dommages … économiques considérables*' or '*une déficience des infrastructures critique avec des conséquences significatives*'.[115]

An objection that is often raised in this context is that a cyber attack that shuts down economic targets such as the stock exchange and disrupts financial markets amounts to economic coercion and not to armed force.[116] This is not correct, for two reasons. First, economic coercion does not have a specific target, while the cyber attack would be undertaken against an identifiable infrastructure. Secondly, while economic coercion, such as an oil embargo, employs the economy as a means of pressure, in a cyber attack that incapacitates the financial market or cripples a State's banking system the economy is rather the target, while the means employed is malware. Therefore, if the stock exchange or other financial institutions were to be bombed kinetically and the markets disrupted as a consequence, this would certainly be considered a use of armed force, and not economic coercion, even though the economic consequences of the action would probably outweigh the physical damage to the buildings: one cannot see why the same conclusion should not apply when the stock exchange, instead of being bombed, is shut down for an extended period of time by a virus in its computer system.[117] Such scenario would arguably be seen as having more in common with a surgical kinetic attack than with the 1973 Organization of the Petroleum Exporting Countries (OPEC)'s oil embargo. If, however, the disruption caused is not severe, 'the cyber attack may be less likely to be regarded as a use of force than a kinetic attack with the same (temporary) economic effect, simply because the lack of physical destruction would reduce the scale of the damage caused'.[118]

It should be stressed again that, if *all* cyber attacks that employ capabilities resulting in damage to physical property or persons are a use of force, those without physical consequences fall under the scope of Article 2(4) only when they go beyond mere inconvenience and cause *significant* disruption of essential services by rendering ineffective or unusable critical infrastructure.[119] It is only in these cases that the effects of loss of functionality can be equated to those of destruction caused by traditional armed force. A week-long cyber attack

---

[113] Keynote address by the Minister of Defence, Ms Ank Bijleveld, marking the first anniversary of the Tallinn Manual 2.0 on the 20th of June 2018 https://english.defensie.nl/downloads/speeches/2018/06/21/keynote-address-by-the-minister-of-defence-ms.-ank-bijleveld-marking-the-first-anniversary-of-the-tallinn-manual-2.0-on-the-20th-of-june-2018 accessed 30 November 2019.

[114] Dutch Minister of Foreign Affairs (n 13) 4.

[115] Ministère des Armées (n 10) 7, 9. The document suggests that the following non-exhaustive and non-binding factors should be taken into account when considering whether the cyber operation qualifies as a use of force: '*l'origine de l'opération et la nature de l'instigateur (son caractère militaire ou non), le degré d'intrusion, les effets provoqués ou recherchés par l'opération, ou encore la nature de la cible visée*'; ibid., 7).

[116] See e.g., Elizabeth Wilmshurst, 'The Chatham House Principles of international law on the use of force in self-defence' (2006) 55 *Intl and Comparative L Quarterly* 963, 965.

[117] Brown and Poellet (n 102) 138; Lin (n 64) 74.

[118] Lin ibid., 74.

[119] Vida M Antolin-Jenkins, 'Defining the parameters of cyberwar operations: Looking for law in all the wrong places?' (2005) 51 *Naval L Rev* 132, 172; Ziolkowski (n 91) 74–5.

that shuts down the national grid, and thus leaves millions of people without electricity, cripples the financial market and the transport system, and prevents government communications is likely to be treated as a use of force, whether or not physical damage ensues.[120] On the other hand, a cyber attack that shuts down a university network is not a use of force, even if it causes prolonged and severe service disruption, because the services affected are not critical.

Those worried that, by qualifying certain cyber operations resulting in loss of functionality as a use of force, the risk of inter-State conflicts will increase should be reassured: indeed, a use of force, in itself, is not sufficient to entitle the victim State to react in self-defence, unless it is serious enough to amount to an 'armed attack'.[121] Apart from the stigma attached to it, then, the only consequence of qualifying cyber operations resulting in the significant disruption of essential services as a use of force is that they could not be undertaken in countermeasure, which certainly is a welcome result, considering the severe negative impact that they might have on the public order of today's digitally reliant societies.[122]

(c) Other Cyber Attacks

Cyber attacks not resulting, or not reasonably likely to result, in physical damage to property or persons, or significant loss of functionality of physical infrastructures, are not a use of force and are therefore not a violation of Article 2(4) of the UN Charter: when attributed to a State, however, they can amount to a violation of the principle of non-intervention in the internal affairs of another State.[123] According to the ICJ, the principle of non-intervention is 'part and parcel of customary international law'.[124] Intervention is 'the manifestation of a policy of force'[125] and is characterised by the element of coercion: a State exercises abusive pressure on another State in order to compel it, through certain means, to do or not to do something 'on matters in which each State is permitted, by the principle of State sovereignty, to decide freely', such as 'the choice of a political, economic, social and cultural system, and the formulation of foreign policy'.[126]

In *Nicaragua*, the ICJ also found that intervention can occur 'with or without armed force'.[127] Indeed, in the Cold War attempts were made to broaden the principle of non-intervention so to

---

[120] The scenario is inspired by the 'Cyber ShockWave' simulation staged by the Bipartisan Policy Center (Ellen Nakashima, 'War game reveals U.S. lacks cyber-crisis skills', *The Washington Post* (17 February 2010) https://www.pressreader.com/usa/the-washington-post/20100216/282857957068734 accessed 30 November 2019).

[121] *Nicaragua Case* (n 2) para 249.

[122] Art 50(1)(a) of the ILC Articles on the Responsibility of States for Internationally Wrongful Acts, *Ybk of the ILC*, 2001, vol II, Part Two, 30.

[123] Dutch Minister of Foreign Affairs (n 13) 4.

[124] *Nicaragua Case* (n 2) para 202.

[125] *Corfu Channel (United Kingdom v Albania)* (Merits, Judgment) [1949] ICJ Rep 4, 35.

[126] *Nicaragua Case* (n 2) para 205. According to the ICJ, '[i]ntervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion … defines, and indeed forms the very essence of, prohibited intervention' (ibid). See Maziar Jamnejad and Michael Wood, 'The principle of non-intervention' (2009) 22 *Leiden J of Intl L* 345–81. The Dutch Minister of Foreign Affairs has defined coercion as 'compelling a state to take a course of action (whether an act or an omission) that it would not otherwise voluntarily pursue' (Dutch Minister of Foreign Affairs (n 13) 3).

[127] *Nicaragua Case* (n 2) para 206.

include economic coercion as a consequence of the increased cooperation among States allowing more subtle ways of interference than the use of force:[128] a further broadening of the notion to include at least certain cyber operations is now necessitated by the interconnectivity of networks and the reliance of modern societies on information systems. All in all, whether a cyber operation below the use of force threshold amounts to an unlawful intervention depends on whether it is used 'to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind' in a matter falling within its domestic jurisdiction.[129] The UK Attorney-General, for instance, qualified cyber attacks 'in the fundamental operation of Parliament, or in the stability of [the UK's] financial system' as a clear breach of the principle of non-intervention.[130] If it was proved that Russia was responsible for the attacks, the 2006 DDoS attacks on Estonia would also be a good illustration of an unlawful intervention conducted by cyber means, as it is suspected that the attacks were intended to coerce the Baltic State into reversing its decision to move a Russian war memorial statue to the suburbs of Tallinn.[131] Ransomware attacks, examples of which are the May 2017 WannaCry cyber attack, which disrupted, among others, the health service's networks in the UK for a few days,[132] and the subsequent NotPetya attack, which affected government agencies and the shipping, power and healthcare sectors in several countries,[133] are another type of cyber operations characterised by coercion: the hacker hijacks a system so that its owner cannot have access to it unless they submit to the hacker's requests (normally the payment of a sum of money in bitcoins, but nothing excludes more political demands to extort undue advantages).

It is not only State-sponsored cyber attacks causing loss of functionality of physical infrastructures or preventing access to systems that can constitute a violation of the principle of non-intervention, but also those engaged in propaganda through web defacement or other methods. Indeed, a State's cyber operation that coerces a public or private website hosted on servers located in another State into deleting or replacing certain content amounts to an unlawful intervention in the affairs of the State of the server, as the regulation of website content falls within each State's domestic jurisdiction.[134] The violation of the principle of non-intervention is particularly evident when the predominant purpose of cyber propaganda is to foment civil strife in another State. In September 2012, for instance, Azerbaijan denounced cyber

---

[128] Philip Kunig, 'Intervention, Prohibition of', *Max Planck Encyclopedia* (n 25) vol. VI, 290.

[129] Declaration on Friendly Relations, UNGA Res 2625 (XXV) (24 October 1970) third principle. See UNGA Res 2131 (XX) (21 December 1965) para 2.

[130] Cyber and International Law in the 21st Century (n 17).

[131] Buchan (n 31) 225–6.

[132] The attack lasted three days, during which it infected the systems of private enterprises and governmental institutions, and was allegedly conducted by a North Korean hacker, Lazarus. See Cyber and International Law in the 21st Century (n 17).

[133] The attack took place in June 2017. See Michael N Schmitt and Jeffrey Biller, 'The NotPetya cyber operation as a case study of international law' (11 July 2017) EJIL: *Talk!* https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/ accessed 30 November 2019. It seems that, even though it spread globally, the attack was aimed at Ukraine and 'was probably launched by a state actor or a non-state actor with support or approval from a state' (CCDCOE, 'NotPetya and WannaCry call for a joint response from international community' (30 June 2017) https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/ accessed 30 November 2019.

[134] *Tallinn Manual 2.0* (n 70) 315–6.

attacks conducted by a so-called 'Armenian Cyber Army' under the 'direction and control' of Armenia that were 'aimed at glorifying terrorists and insulting their victims, as well as at advocating, promoting and inciting ethnically and religiously motivated hatred, discrimination and violence'.[135]

In the specific context of a non-international armed conflict, the principle of non-intervention also prohibits all cyber operations that aim at supporting directly or indirectly an armed opposition group, even when they do not directly cause physical damage or loss of functionality of infrastructures in the target State.[136] The hacker group Fancy Bear, for instance, has been accused of infecting an 'app' used by the Ukrainian armed forces in the military operations against secessionist insurgents in Eastern Ukraine: this allegedly allowed the Russian forces to access phone communications and localization data of the Ukrainian artillery, thus facilitating attacks against Ukraine's forces.[137] Fancy Bear is suspected of being affiliated with the Russian military intelligence agency.

(d) Conduct Related to Cyber Attacks

It has already been seen that, according to the ICJ, it is not only the direct use of weapons by a State against another State that amounts to a use of force, but also enabling someone else to use those weapons: the arming and training of armed groups, therefore, is a violation of Article 2(4), even though not an armed attack.[138] If this view is extended to the cyber context, one must conclude that the supply of malware by a State to an armed group acting against another State and the training of such group to conduct cyber attacks are also a use of force.[139] This is the *opinio juris* of France.[140] This conclusion, however, is correct only when the supply of malware and the training enable the group to conduct cyber attacks amounting to a use of force, and not cyber operations below that threshold.

Similarly, if one transposes Article 3(f) of the Definition of Aggression in cyberspace, a State that knowingly allows another State to use its cyber infrastructure in order to launch a cyber attack amounting to an act of aggression against a third State would commit an act of aggression itself, and therefore would breach the prohibition of the use of force.[141] It appears, for instance, that North Korea's cyber warfare Unit 121 is at least partially stationed in China due to the limited internet connections in North Korea, although the involvement of

---

[135] Letter dated 6 September 2012 from the Chargé d'affaires a.i. of the Permanent Mission of Azerbaijan to the United Nations addressed to the Secretary-General (7 September 2012) UN Doc A/66/897–S/2012/687, 1.

[136] Cfr *Nicaragua Case* (n 2) para 246.

[137] Matteo Fornari, 'Conflitto in Ucraina, orsi fantasiosi e programmi malevoli' (2017) 100 *Rivista di Diritto Internazionale* 1156, 1156–7.

[138] *Nicaragua Case* (n 2) para 228.

[139] An example is the alleged cyber training of members of the Syrian opposition by the US State Department (Jay Newton-Small, 'Inside America's secret training of Syria's digital army', *Time* (13 June 2012) http://swampland.time.com/2012/06/13/inside-americas-secret-training-of-syrias-digital-army accessed 30 November 2019).

[140] Ministère des Armées (n 10) 7.

[141] Art 3(f) of the Definition of Aggression includes among the acts of aggression: '[t]he action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State'.

the Chinese Government is unclear.[142] Article 3(f), however, would only potentially apply to situations where the cyber operation in question amounts to an act of aggression, not to any use of force and even less to cyber operations below that threshold.

On the other hand, according to the ICJ, the 'mere supply of funds' to armed groups does not amount to a use of force, although it 'undoubtedly' qualifies as unlawful intervention.[143] A State that funds the cyber operations of an armed group against another State, therefore, may breach the principle of non-intervention in the internal affairs of that State, but not Article 2(4).[144]

4. CONCLUSIONS

The provisions on the use of force contained in the UN Charter apply to cyber operations even though they were adopted well before the advent of cyber technologies: the lack of ad hoc rules does not mean that cyber operations may be conducted by States against other States without restrictions. This chapter has argued that a cyber operation is a use of armed force when it entails the use of a 'weapon' accompanied by a coercive intention. This occurs not only in the case of cyber attacks designed to cause physical damage to property, loss of life or injury of persons, but also of cyber attacks employing capabilities that render ineffective or unusable critical infrastructures so to cause *significant* disruption of essential services, even when they do not materially damage those infrastructures. Indeed, the digitalization of today's societies has made it possible to cause considerable harm to States through non-destructive means: physical infrastructures can be disabled by affecting their operating systems, with consequent disruption of services but without the need to destroy them. An evolutionary interpretation of Article 2(4) should take this into account.

As to cyber attacks conducted by States but falling below the level of the use of force, i.e., those that do not result in material damage to property or persons or severe disruption of essential services, they can constitute a violation of the principle of non-intervention in the internal affairs of other States if they are 'the manifestation of a policy of force',[145] i.e., if they are accompanied by an intention to coerce the target State to do or not to do something 'on matters in which each State is permitted, by the principle of State sovereignty, to decide freely'.[146] On the other hand, cyber espionage can be a violation of the sovereignty of the targeted State when it entails an unauthorized intrusion into the cyber infrastructure located on its territory, but not an intervention and even less a use of force, as it lacks the coercive element and does not normally involve the use of a weapon, i.e., a payload capable of resulting in physical damage or malfunction of infrastructures. When it does, it becomes (also) a cyber attack and the considerations made in relation to such operations will apply.

---

[142] Richard A Clarke and Robert K Knake, *Cyber War. The Next Threat to National Security and What To Do About It* (Harper Collins 2010) 27–8.

[143] *Nicaragua Case* (n 2) para 228.

[144] Michael N Schmitt, 'The law of cyber warfare: *Quo vadis*?' (2014) 25 *Stanford L and Policy Rev* 269, 280.

[145] *Corfu Channel* (n 125) 35.

[146] *Nicaragua Case* (n 2) para 205.

15. Self-defence in cyberspace

Carlo Focarelli

1. INTRODUCTION

Self-defence is permitted under Article 51 of the United Nations (UN) Charter and customary international law, as the ICJ stated in the *Nicaragua Case*.[1] Article 51 reads:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.[2]

In the system of the Charter the right of self-defence basically allows a State, either individually or collectively, to respond militarily to an armed attack until the UN Security Council takes measures necessary to maintain international peace and security. Self-defence thus clearly constitutes an exception to the general prohibition on the threat and use of force set out in Article 2(4) UN Charter.

The question as to whether the international law rule on self-defence applies to cyber attacks is much debated. No explicit international law rules exist specifically applicable to self-defence in cyberspace and the law of self-defence predates the advent of cyber operations. A treaty on cyber operations is unlikely in the foreseeable future, one of the reasons being that the most vulnerable States are at the same time those most capable of conducting cyber attacks.[3] A treaty for cyber disarmament has been proposed by the Russian Federation, but opposed by the United States[4] and fiercely resisted by the private commercial cyber sector as early as at the 2012 World Conference on International Telecommunications.[5] As a result the

---

[1] *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States),* Judgment (Merits) [1986] ICJ Rep 14, para 176.

[2] On Article 51 see Bruno Simma, Daniel-Erasmus Khan, Georg Nolte and Andreas Paulus (eds), *The Charter of the United Nations: A Commentary* (OUP 2012).

[3] Michael N Schmitt, 'Cyber operations and the jus ad bellum revisited' (2011) 56 *Villanova L Rev* 569, 604.

[4] John Markoff and Andrew E Kramer, 'US and Russia differ on a Treaty for Cyberspace', *New York Times* (27 June 2009) https://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all accessed 7 February 2020. It has been observed that the US plans to use the Internet for offensive purposes, as it is believed it has done with Stuxnet (see section 4 below): *cf* Mary Ellen O'Connell, 'Cyber security without cyber war' (2012) 17 *J of Conflict & Security L* 187, 206; François Delerue, *Cyber Operations and International Law* (CUP 2020).

[5] See Myjer (Ch 17 of this Handbook); David Gross and Ethan Lucarelli, 'The 2012 World Conference on International Telecommunications: Another brewing storm over potential UN regulation of the internet', *Who's Who Legal* (30 April 2012) https://whoswholegal.com/features/features/the-2012

question translates into asking whether and to what extent the rules applying to physical (or 'kinetic') armed attacks also apply to cyber attacks.

While this chapter is confined to self-defence, there are at least two connections between the use of force in cyberspace discussed in the previous chapter and armed attacks analysed here worth considering: first, there can be no cyber armed attack justifying self-defence when such an attack does not amount to a 'use of force' in the first place; secondly, a cyber counter-attack in self-defence may exceed the limitations imposed by law to the right of self-defence and become an unlawful 'use of force'.

Finally, some terminological observations are in order before addressing the issue of self-defence in cyberspace. The term 'cyber', coming from 'cybernetics', is usually linked with 'space'. The idea of 'cyberspace', associated with McLuhan's image of the 'global village' and William Gibson's state of 'consensual hallucination',[6] is found in the well-known 'Declaration of the Independence of Cyberspace' made by John Barlow in 1995, defining cyberspace as a space which 'does not lie within [States'] borders' and 'a world that is both everywhere and nowhere'.[7] It has been noted, however, that cyberspace is not a space at all.[8] Cyberspace is 'no more than the interconnection of electronic pathways',[9] a technology of inter-connection between people who are located in the *physical* world, under the authority of one or more *States*, this inter-connection being possible by a *physical* infrastructure which is predominantly made up of trans-ocean fibre optic cables and, to a small extent, of satellites.[10]

2. TOPICALITY OF CYBER SECURITY

States are increasingly going on line and their critical national infrastructure is more and more controlled by networked computer systems, especially in technologically advanced societies. In doing so, States seek to gain a comparative advantage and be more competitive but this makes them increasingly vulnerable and they must 'patrol' cyberspace to prevent cyber threats and to respond timely and effectively to such threats. States appear to be willing to use cyberspace, accept its risks but at the same time militarize cyberspace in order to respond to

---

-world-conference-on-international-telecommunications-another-brewing-storm-over-potential-un-regulation-of-the-internet1 accessed 7 February 2020; David Meyer, 'ITU chief claims Dubai meeting "Success", despite collapse of talks', *ZDnet* (14 December 2012) https://www.zdnet.com/article/itu-chief-claims-dubai-meeting-success-despite-collapse-of-talks accessed 7 February 2020.

[6] Marshall McLuhan, *Understanding Media: The Extensions of Man* (Gingko Press 1964) 6; William Gibson, *Neuromancer* (Ace Books 1984) 69.

[7] https://www.eff.org/cyberspace-independence accessed 7 February 2020.

[8] Mark Graham, 'Time machines and virtual portals: The spatialities of the digital divide' (2011) 11 *Progress in Development Studies* 215, https://journals.sagepub.com/doi/pdf/10.1177/146499341001100303 accessed 7 February 2020; Mark Graham, 'Cyberspace', *ZeroGeography* (3 November 2011) http://www.markgraham.space/blog/cyberspace accessed 7 February 2020.

[9] US Supreme Court, *Reno v. American Civil Liberties Union*, 521 U.S. 844, 889–90 (1997). According to the US Department of Defense cyberspace is 'a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers' (US Department of Defence, 'Quadrennial Roles and Missions Review Report' (January 2009) 15.

[10] See TeleGeography, 'The Submarine Cable Map' https://www.submarinecablemap.com accessed 7 February 2020.

cyber threats. A few data taken from recent international practice may illustrate the topicality of cyber security today.

According to the International Telecommunication Union (ITU) '[a]t the end of 2018, 51.2 per cent of individuals, or 3.9 billion people, were using the Internet'.[11] In 2019 the number of attack groups using destructive malware to destroy and disrupt business operations grew 25 per cent.[12] Since 2007 ITU has been working on its *Global Cyber-security Agenda* and in 2011 it entered into an agreement with the International Multilateral Partnership Against Cyber Threats (IMPACT), an international public-private initiative dedicated to enhancing the global community's capacity to prevent, defend and respond to cyber threats. The 2011 ITU 'National Cybersecurity Strategy Guide' presented a 'National Cybersecurity Strategy Model' together with, inter alia, an overview of legal, technical and procedural measures.[13]

Since 2001 up to December 2018 the UN General Assembly has adopted a number of resolutions noting that 'the dissemination and use of information technologies and means affect the interests of the entire international community'. At the same time, the General Assembly warned that 'these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields'.[14]

NATO expressly referred to cyber security in its 2010 Strategic Concept. It noted that it will 'develop further its ability to prevent, detect, defend against and recover from cyber-attacks'.[15] Every year, since 2008, a high-level NATO Cyber Conference has been organized in Tallinn (Estonia) by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE),[16] the latest Conference having been held in June 2019.[17] The Centre has drafted, inter alia, a 'Manual on the International Law Applicable to Cyber Warfare', published in 2013, and, in

---

[11] ITU, 'Measuring the Information Society 2018' https://www.itu.int/pub/D-IND-ICTOI accessed 7 February 2020.

[12] Symantec 'Internet Security Threat Report 2019', *Symantec* (February 2019) https://www.symantec.com/security-center/threat-report accessed 7 February 2020.

[13] For the latest issue, see 'ITU National Cybersecurity Strategy Guide' (ITU 2018) https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018 accessed 7 February 2020.

[14] UNGA Res 56/19, 'Developments in the field of information and telecommunications in the context of international security' (7 January 2002). See subsequently UNGA Res 58/32 (18 December 2003); UNGA Res 59/61 (3 December 2004); UNGA Res 60/45 (8 December 2005); UNGA Res 61/54 (6 December 2006); UNGA Res 62/17 (5 December 2007); UNGA Res 63/37 (2 December 2008); UNGA Res 64/25 (2 December 2009); UNGA Res 65/41 (8 December 2010); UNGA Res 66/24 (2 December 2011); UNGA Res 67/27 (3 December 2012); UNGA Res 68/243 (27 December 2013); UNGA Res 69/28 (2 December 2014); UNGA Res 70/237 (23 December 2015); UNGA Res 71/28 (5 December 2016); UNGA Res 73/27 (5 December 2018), Res 73/187 (17 December 2018) and Res 73/266 (22 December 2018). On the role of the UN in cyber security see Henderson (Ch 28 of this Handbook).

[15] 'Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted by Heads of State and Government at the NATO Summit in Lisbon (19–20 November 2010) para 19 http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf accessed 7 February 2020.

[16] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) https://ccdcoe.org accessed 7 February 2020.

[17] CyCon 2019 (11th International Conference on Cyber Conflict: Silent Battle) 28-31 May 2019, proceedings at https://ccdcoe.org/uploads/2019/06/CyCon_2019_BOOK.pdf accessed 7 February 2020.

2017, it published the Tallinn Manual 2.0.[18] The 2012 Chicago Summit Declaration reiterated the commitment of member States to 'develop further our ability to prevent, detect, defend against, and recover from cyber attacks'.[19]

Since 2008 many States, in addition to the European Union, have developed National Strategies and Policies concerning cybersecurity.[20] An increasing number of States are also establishing intelligence or military cyber units and commands to address cyber threats.[21] For example, in 2004 the European Network and Information Security Agency (ENISA) was established as a body devoted to achieving a high and effective level of network and information security within the EU.[22] In the US, in January 2008 US President George W Bush launched the 'Comprehensive National Cybersecurity Initiative' (CNCI).[23] In 2010 the US Department of Defense established Cyber Command, as a sub-unit of Strategic Command, with a view to being prepared 'to respond to hostile acts in cyberspace' and, accordingly, to reserving 'the right, under the laws of armed conflict, to respond to serious cyber-attacks, with a proportional and justified military response, at the time and place of its choosing.[24] In May 2011 US President Obama stated that 'the United States will respond to hostile acts in cyberspace' since '[a]ll states possess an inherent right to self-defense', thus reserving 'the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law'.[25] The same year the Obama Administration concluded that '[t]hreats to cyberspace pose one of the most serious economic and national security challenges of the 21st Century for the United States and our allies'.[26] In 2012 the Secretary of the US Department of Homeland Security (DHS) called for cyber-security intelligence information sharing with private sector companies as critical infrastructure providers (such as gas companies, water suppliers, etc.) 'which are at constant risk of cyber-attack'.[27]

[18] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017).

[19] Chicago Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago (20 May 2012) para 49 https://www.nato.int/cps/en/natolive/official_texts_87593.htm#cyber accessed 7 February 2020. On NATO and cyberspace see Hill (Ch 24 of this Handbook).

[20] On the role of the EU in cyber security see Wessel (Ch 23 of this Handbook); ITU, 'Guide to developing a national cybersecurity strategy—Strategic engagement in cybersecurity' https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx accessed 7 February 2020.

[21] E.g., US Cyber Command (USCYBERCOM).

[22] ENISA was set up by Regulation (EC) No 460/2004 of the European Parliament and of the Council on 10 March 2004. For further information, see https://www.enisa.europa.eu.

[23] National Security Council, *The Comprehensive National Cybersecurity Initiative* (2009) https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative accessed 7 February 2020.

[24] William Lynn, 'Announcement of the Department of Defense Cyberspace Strategy at the National Defense University' (U.S. Department of Defense, 14 July 2011) https://archive.defense.gov/speeches/speech.aspx?speechid=1593 accessed 7 February 2020.

[25] White House, 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World' (Washington, May 2011) https://info.publicintelligence.net/WH-International Cyberspace.pdf accessed 7 February 2020.

[26] White House, 'Cyberspace Policy Review: Assuring a trusted and resilient information and communications infrastructure' (Washington, 2009) https://www.energy.gov/sites/prod/files/cioprod/documents/Cyberspace_Policy_Review_final.pdf accessed 30 November 2013.

[27] Eric B Parizo, 'Napolitano calls for cybersecurity intelligence information sharing', *TechTarget* (10 September 2012) https://searchsecurity.techtarget.com/news/2240162981/Napolitano-calls-for-cybersecurity-intelligence-information-sharing accessed 7 February 2020.

Most recently, in the 2018 'National Cyber Strategy' US President Donald Trump stated his determination to:

> [d]efend the homeland by protecting networks, systems, functions, and data; [p]romote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; [p]reserve peace and security by strengthening the ability of the United States—in concert with allies and partners—to deter and, if necessary, punish those who use cyber tools for malicious purposes; and [e]xpand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet.[28]

A similar concern has also been raised within NATO.[29]

3. KEY CASES THUS FAR

While cyber attacks, broadly defined, are very frequent (and routinely reported, for example, by Symantec and McAfee, two respected anti-virus companies), very few cyber attacks have made headlines thus far as 'attacks on states' and have been cited in military security discussions. A few words on some well-known cases recently occurred (concerning Estonia in 2007, Syria in 2007, Georgia in 2008, Iran in 2010, and a great deal of States in couple of attacks in 2017) may be useful for present purposes.

In April 2007 Estonia, one of the most wired societies in Europe at the time and a pioneer in the development of 'e-government', was paralyzed by a cyber attack for a few weeks.[30] The attack was clearly prompted by the Estonians' relocation of the Soviet World War II memorial. Many critical infrastructures, including the banking system, several government services and much of the media, broke down. The attack consisted of a simultaneous huge number of information requests which overloaded and blocked the entire system (so called 'Distributed denial of service' (DDoS)). Estonian authorities referred the case to NATO adumbrating the notion that NATO should have reacted as a matter of Article 5 of the North Atlantic Treaty.[31] NATO, however, rejected the claim. A NATO official simply said that: 'This is an operational security issue, something we're taking very seriously.' Mr Jaak Aaviksoo, the Estonian Defence

---

[28] The White House, 'National Cyber Strategy of the United States of America' (20 September 2018) https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[29] See NATO, 'Working with the private sector to deter cyber attacks' (10 November 2011) https://www.nato.int/cps/en/natolive/news_80764.htm accessed 7 February 2020.

[30] See e.g., Mark Landler and John Markoff, 'Digital fears emerge after data siege in Estonia', *New York Times* (29 May 2007) https://www.nytimes.com/2007/05/29/technology/29estonia.html accessed 7 February 2020.

[31] Article 5 NATO reads:

> The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.

Minister who had raised the matter with NATO, acknowledged that: 'At present, NATO does not define cyber-attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defence, will not automatically be extended to the attacked country', adding that, 'Not a single NATO defence minister would define a cyber-attack as a clear military action at present'.[32] The Russian Federation was suspected of being behind the attack, but it denied any involvement and there is no conclusive evidence suggesting that it was actually involved.[33]

In September 2007, Israel supposedly disabled the Syrian networked air defence system when its air force penetrated the Syrian air space and bombed a suspected nuclear site without being engaged or even detected.[34]

In August 2008, a number of cyber attacks hit Georgia immediately before and during the Russian occupation of Ossetia. This prevented the Georgian authorities from keeping information flowing to the national and international media. The Russian Federation was immediately suspected, but in this case too there is no conclusive evidence of its actual involvement.[35] As is apparent, in both the Syrian case and in the Georgian case, unlike the Estonian case, cyber attacks preceded and/or accompanied a *conventional* attack.

In June 2010 a malware (i.e., a malicious software, a 'worm' in this case) called 'Stuxnet' hit approximately 1,000 centrifuges at Iran's Natanz nuclear enrichment facility, in addition to thousands of other computers elsewhere in the world. Stuxnet targeted industrial control systems, known as programmable logic controllers (PLCs), made by Siemens. In this case, Israel and the US were suspected of the attack,[36] but, once again, without any conclusive evidence (although recently there have been revelations confirming this allegation). Iran also accused the German engineering firm Siemens of helping Israel and the US launch Stuxnet by providing information about a Siemens-designed control system (SCADA) used in Iran's nuclear sites.[37] Neither the US and Israel have denied computer experts' claims that

---

[32] Ian Traynor 'Russia accused of unleashing cyberwar to disable Estonia', *The Guardian* (Brussels, 17 May 2007 Brussels https://www.theguardian.com/world/2007/may/17/topstories3.russia accessed 7 February 2020.

[33] Joshua Davis, 'Hackers take down the most wired country in Europe', *Wired Magazine* (21 August 2007) https://www.wired.com/2007/08/ff-estonia/?currentPage=all accessed 7 February 2020.

[34] Richard A Clarke and Robert K Knake, *Cyber War: The Next Threat to National Security and What To Do about It* (Harper Collins 2010) 1–8.

[35] Jon Swaine, 'Georgia: Russia "conducting cyber war"', *The Telegraph* (11 August 2008) https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html accessed 7 February 2020; Lesley Swanson, 'The era of cyber warfare: Applying international humanitarian law to the 2008 Russian-Georgian conflict' (2010) 32 *Loyola of Los Angeles Intl and Comparative L Rev* 303; Eneken Tikk and others, *Cyber Attacks Against Georgia: Legal Lessons Identified* (CCDCOE 2008).

[36] William J Broad, John Markoff and David E Sanger, 'Israeli test on worm called crucial in Iran nuclear delay', *New York Times* (15 January 2011) https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all accessed 7 February 2020; Johnatan Fildes, 'Stuxnet work "Targeted high-value Iranian assets"', *BBC News* (23 September 2010) https://www.bbc.com/news/technology-11388018 accessed 7 February 2020; James Hider, 'Computer virus used to sabotage Iran's nuclear plan "built by US and Israel"', *The Australian* (17 January 2011) https://www.theaustralian.com.au/news/world/computer-virus-used-to-sabotage-irans-nuclear-plans-built-by-us-and-israel/news-story/08eaf40536d1a14ca4fb39db2d396e7e accessed 7 February 2020.

[37] Saeed K Dehghan, 'Iran accuses Siemens of helping launch Stuxnet cyber-attack', *The Guardian* (17 April 2011) https://www.theguardian.com/world/2011/apr/17/iran-siemens-stuxnet-cyber-attack?INTCMP=SRCH accessed 6 February 2020.

they were behind the development of Stuxnet. In October 2011, Stuxnet's successor, Duqu, came to light. It uses a zero-day exploit to install spyware that records keystrokes and other system information.[38] In the Iranian case the cyber attack, like in the Estonian case, was not accompanied by a conventional attack; however, unlike in the Estonian case, it was caused by a malware rather than by a DDoS.

In May 2017 WannaCry, a ransomware cryptoworm cyber attack, targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It exploited a known vulnerability in older Windows systems called EternalBlue, which was found by the US National Security Agency (NSA). The attack was halted within a few days of its discovery due to emergency patches released by Microsoft and the discovery of a kill switch that prevented infected computers from spreading WannaCry further. The attack was estimated to have affected in a few hours more than 200,000 computers across 150 States, with total damages ranging from hundreds of millions to billions of dollars. In December 2017, the US, the UK and Australia formally asserted that North Korea was behind the attack.[39]

Finally, in June 2017, a new variant of Petya—a family of encrypting ransomware that was first discovered in March 2016—was used for a global cyber attack, primarily targeting Ukraine. It also propagated via the EternalBlue exploit, with damages estimated at more than $10 billion. On 15 February 2018, the Trump administration blamed Russia for the attack and warned that there would be 'international consequences',[40] just as the UK and Australia did.[41]

These cases have been differently assessed in legal terms in the literature. For example, Lucas argues for the justifiability of the Syrian, Georgian, and Stuxnet cases and the unjustifiability of the Estonian case in the light of the just war doctrine.[42] O'Connell denies that all such attacks amounted to the equivalent of an Article 51 'armed attack'.[43] Buchan argues that while Stuxnet did cause damage capable of establishing a violation of Article 2(4) UN Charter, the Estonia case was one of a violation of the principle of non-intervention.[44] According to Tsagourias neither the Estonian nor the Georgian case fell within the definition of armed attack for self-defence purposes since the disruption they caused was contained and manageable.[45]

---

[38] Symantec (n 12).

[39] Thomas P Bossert, 'It's official: North Korea is behind WannaCry', *The Wall Street Journal* (18 December 2017) https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537 accessed 7 February 2020.

[40] Morgan Chalfant 'Trump admin blames Russia for massive global cyberattack', *The Hill* (15 February 2018) https://thehill.com/policy/cybersecurity/374104-trump-admin-blames-russia-for-global-cyberattack-warns-of-international accessed 7 February 2020.

[41] Rafia Shaikh 'US, UK, Australia warn Russia of "International Consequences"—NotPetya outbreak attributed to the Kremlin', *Wccftech* (16 February 2018) https://wccftech.com/australia-us-uk-russia-notpetya accessed 7 February 2020.

[42] George R Lucas, 'Permissible preventive cyberwar: Restricting cyber conflict to justified military targets' in Luciano Floridi and Mariarosaria Taddeo (eds), *Philosophy of Engineering and Technology* (UNESCO Conference on Ethics and Cyber Warfare, University of Hertfordshire, 1 July 2011); Randall R Dupert, 'The ethics of cyberwarfare' (2010) 9 *J of Military Ethics* 384.

[43] O'Connell (n 4) 201–2.

[44] Russell Buchan, 'Cyber attacks: Unlawful uses of force or prohibited interventions' (2012) 17 *J of Conflict and Security L* 211, 225–6.

[45] Nicholas Tsagourias, 'Cyber attacks, self-defence and the problem of attribution' (2012) 17 *J of Conflict and Security L* 229, 232.

4. PREVAILING APPROACHES TO CYBER THREATS IN LEGAL DOCTRINE

The key issue in the cyber attack debate is about whether cyber security should be ensured by militarizing cyberspace and being prepared to respond kinetically if necessary or by relying on 'civil' law enforcement measures. Most commentators on the international law applicable to cyber war scenarios are in fact experts on the use of force and often closely tied to the military.

It is first to be noted that a number of commentators argue that international law has (or should have) no role at all in cyber security because it would leave the military 'unable to fight, or even to plan for, a war in cyberspace'.[46] Others find it difficult to apply the existing rules of international law concerning the use of force by way of analogy to cyber operations and argue for an 'updated' looser interpretation of such rules so as to apply in the cyber context, often resuming an approach furthered during the Cold War in relation to nuclear deterrence.[47] Still others reply that the better analogy is with the law enforcement paradigm managed by civil authorities applying to maritime piracy or to chemicals used as weapons.[48] Yet others have no doubt that international law, including its rules on the use of force, applies to cyber space.[49] For example, in a speech delivered on 23 May 2018, UK Attorney General Jeremy Wright emphasised that 'it is the UK's view that there are boundaries of acceptable state behaviour in cyberspace, just as there are everywhere else' and that 'cyber space is an integral part of the rules based international law'. Likewise, in its 2013 report the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security pointed out that '[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment'.[50]

---

[46] Stewart A Baker and Charles J Dunlap, 'What is the role of lawyers in cyberwarfare?', *ABA Journal* (1 May 2012) http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare accessed 7 February 2020; Stewart A Baker, 'Denial of service, against cyberwar with arcane rules and regulations', *Foreign Policy* (30 September 2011) https://foreignpolicy.com/2011/09/30/denial-of-service accessed 7 February 2020.

[47] Matthew C Waxman, 'Cyber-attacks and the use of force: Back to the future of Article 2(4)' (2011) 36 *Yale J of Intl L* 421. See previously Mike McConnell, 'To win the cyber-war, look to the Cold War', *Washington Post* (8 February 2010) B 1 https://www.twincities.com/2010/03/07/mike-mcconnell-to-win-the-cyber-war-look-to-the-cold-war accessed 30 November 2013; Mike McConnell, 'How to win the cyber war we are losing', *Washington Post* (28 February 2010) https://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html accessed 7 February 2020.

[48] Noah Schachtman and Peter Singer, 'The wrong war: The insistence on applying Cold War metaphors to cybersecurity is misplaced and counterproductive', *Brookings* (15 August 2011) https://www.brookings.edu/articles/the-wrong-war-the-insistence-on-applying-cold-war-metaphors-to-cybersecurity-is-misplaced-and-counterproductive accessed 7 February 2020; Ryan Singel, 'White House Cyber Czar: "There is no cyberwar"', *Wired Magazine* (4 March 2010) https://www.wired.com/2010/03/schmidt-cyberwar accessed 7 February 2020.

[49] UK Attorney General Jeremy Wright, 'Cyber and International Law in the 21st Century' speech made at Chatham Royal Institute for International Affairs on 23 May 2018 https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century accessed 7 February 2020.

[50] UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of 7 June 2013, UN Doc A/68/98, para 19 https://undocs.org/A/68/98 accessed 7 February 2020.

The typical general approach adopted in the international law literature with regard to major cyber threats is whether *jus ad bellum* applies,[51] or whether and to what extent *jus in bello* applies,[52] with some authors covering both fields.[53] Some scholars endeavour to stretch existing rules to cyber attacks by assuming that new treaties are unlikely and perhaps undesirable; while others call for new rules, given the unprecedented nature of cyber weapons. Most studies come from US scholars[54] and often analogize international law so as to apply it to cyber warfare,[55] with few exceptions.[56] Most studies accept that cyber attacks may amount to unlawful 'use of force' prohibited by international law as well as to an 'armed attack' justifying (conventional or 'kinetic') self-defence and to 'armed conflict' capable of triggering the application of international humanitarian law in cases where substantial damage and destruction are caused. While many accept that the effects should be 'comparable' to those of conventional attacks and, in particular, should hit 'critical infrastructure', different views have been taken with respect to the threshold which justifies a military response.

Finally, most studies merely hint at the key issues of identification of the attacker and of legal attribution of the attack to a State.[57] The difference if any between 'cyber crime', 'cyber terrorism' and 'cyber war' remains blurred. Methodology is also rarely addressed.[58]

---

[51] E.g., Marco Roscini, 'World wide warfare: *Jus ad bellum* and the use of cyber force' (2010) 14 *Max Planck Ybk of United Nations L* 85; Schmitt (n 3).

[52] Michael N Schmitt, 'Wired warfare, computer network attack and jus in bello' (2002) *Intl Red Cross Rev* 365; Knut Dörmann, 'Applicability of the Additional Protocols to computer network attacks: An ICRC approach' in Karin Byström (ed), *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law: Proceeding of the Conference* (Swedish National Defence College, 17–9 September 2004); Jenny Döge, 'Cyber warfare: Challenges for the applicability of the traditional laws of war regime' (2010) 48 *Archiv des Völkerrechts* 486; Michael N Schmitt, 'Cyber operations and the jus in bello: key issues' (2011) 41 *Israel Ybk on Human Rights* 113. On the application of IHL to cyberspace see Part IV of this Handbook.

[53] E.g., Michael N Schmitt, 'Computer network attack and the use of force in international law: Thoughts on a normative framework' (1999) 37 *Columbia J of Transnational L* 885; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012).

[54] For an interesting statement by the former US Department of State's Legal Advisor on the US position concerning the role of international law in cyberspace, see Harold H Koh, 'International Law in Cyberspace' (*U.S. Department of State*, USCYBERCOM Inter-Agency Legal Conference, 18 September 2012) https://harvardilj.org/2012/12/online_54_koh accessed 7 February 2020.

[55] Scott J Shackelford, 'From nuclear war to net war: Analogizing cyber attacks in international law' (2008) 27 *Berkeley J of Intl L* 191.

[56] O'Connell (n 4) 209, arguing that 'it is time… to turn to cyber disarmament and a focus on peaceful protection of the Internet' against the growing emphasis in the literature on militarising cyber security.

[57] For a succinct discussion on identification and attribution, see Roscini (n 51) 96–102. See also n 163.

[58] Dinniss (n 53).

5. CYBER ATTACKS AS 'ARMED ATTACKS' UNDER ARTICLE 51 UN CHARTER AND GENERAL INTERNATIONAL LAW

Article 51 mentions 'the inherent right of individual or collective self-defence if an armed attack occurs'. The right of self-defence consists of using armed force unilaterally 'if an armed attack occurs'. For a response to possibly qualify as self-defence, armed force has to be used both by the attacker and by the victim of the attack.

(a) Attacks in Cyberspace

The term 'cyber attack' is perhaps the most commonly used today to describe attacks in cyberspace, but others are often found in the literature, notably 'cyber network attack' (CNA). According to an early definition of the US Department of Defense (Dod), which was routinely accepted as authoritative, a 'Cyber Network Attack', is: '[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves'.[59] More recently, cyberspace attack actions' have been defined by the (Dod) as 'actions [that] create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial effects in the physical domains'.[60] NATO proceeds along similar lines by defining a 'computer network attack' as an '[a]ction taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself', adding that: '[a] computer network attack is a type of cyber attack'.[61] What amounts to an 'attack' in cyberspace is in fact a complex issue for a variety of reasons.[62]

First, not every hostile cyber act is an 'attack' for the purposes of justifying a per se unlawful reaction, let alone a kinetic counter-attack. For example, a DDoS attack is the result of a huge number of apparently 'ordinary' requests for information.[63] It is the number and intent of the

[59] US Department of Defense, 'Dictionary of Military and Associated Terms' (Joint Publication 1-02, 8 November 2010) https://fas.org/irp/doddir/dod/jp1_02-april2010.pdf accessed 7 February 2020.

[60] US Department of Defense, 'Cyberspace Operations' (Joint Publication 3-12, 8 June 2018) https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150 accessed 7 February 2020.

[61] NATO Standardization Agency, 'NATO Glossary of Terms and Definitions' (AAP-6, 2019) 2-C-11 https://nso.nato.int/nso/zPublic/ap/PROM/AAP-06%202019%20EF.pdf accessed 7 February 2020.

[62] The term 'cyber attack' (CA) is perhaps the most commonly used, but others are often found in the literature, in particular Cyber Network Attack (CNA). In the past, Information Warfare (IW) was also used. Other terms, referring to particular operations in the Net, include Information Operation (IO), Cyber Network Exploitation (CNE) and Cyber Network Operation (CNO). See Roscini (n 51) 91–3; Garry D Brown and Owen W Tullos, 'On the spectrum of cyberspace operations' (2012) *Small Wars J*, https://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations accessed 7 February 2020. For sake of brevity I will refer to 'cyber attack' hereinafter. For a general overview, see Michael N Schmitt, '"Attack" as a term of art in international law: The cyber operations context' in Christian Czosseck, Rain Ottis, and Katharina Ziolkowski (eds), *Proceedings of the 4th International Conference on Cyber Conflict* (CCDCOE 2012) 283–93, https://ccdcoe.org/uploads/2019/03/CyCon_book_2012.pdf accessed 7 February 2020.

[63] Hakem Beitollahi and Geert Deconinck, 'A dependable architecture to mitigate distributed denial of service attacks on network-based control systems' (2012) 4 *Intl J of Critical Infrastructure Protection* 107.

master computer rather than one of the controlled computers that make such requests 'hostile'. The question about how 'good' and 'bad' requests can rapidly be distinguished is very difficult and generally requires information from private-sector Internet Service Providers (ISPs) on their traffic, which is usually confidential.

Secondly, there is a variety of potentially relevant cyber attacks that produce very different effects, such as DDoS attacks (as occurred in Estonia and Georgia), malware (as occurred in Iran), so-called 'backdoors' or 'trapdoors' (i.e., undocumented ways of gaining access to a program, online service or an entire computer system for future intrusion), etc. Unlike conventional and nuclear weapons, cyber attacks may have very diverse effects, which may or may not cause destruction, so they cannot be treated as a single homogenous category. For example, a DDoS attack may hit only one single State (as occurred in Estonia), whereas a malware may propagate thorough the global net (as occurred with Stuxnet).

Finally, the difference between a 'cyber attack' amounting to an 'armed attack' (which could possibly justify a military response in self-defence) and 'cyber crime'[64] (which would be treated as an ordinary crime falling within the criminal jurisdiction of one or more States) is often unclear.

(b) 'Use of Force' as Part of an 'Armed Attack'

Under Article 51 UN Charter in order for self-defence to be permitted an 'armed attack' must have occurred. An 'armed attack' for the purposes of Article 51 is a form of 'use of force'[65] under Article 2(4) UN Charter in the first place. Many writers, by adopting a combination of the 'effect-based' (or 'equivalence-based') and the 'target-based' approaches and dismissing the 'instrument-based' approach, have maintained that a cyber attack can constitute a 'use of force' under Article 2(4). It is suggested that what matters is not the 'instrument' used (i.e., the weapon) but rather the effects produced (which have to be approximately equivalent to those produced by conventional weapons)[66] or, for some, the (military or sensitive) target.[67] The term 'force' in Article 2(4) means *armed* force and by 'armed force' is meant, as the ICJ pointed out in the 1996 *Nuclear Weapons* Opinion, 'any use of force, regardless of the weapons employed',[68] supposedly including not only nuclear weapons but also other 'dual-use' weapons such as chemical and biological weapons.[69] Although not being 'armed' in the traditional sense, cyber attacks may thus amount to a 'use of force' under Article 2(4). As such, when amounting to 'aggression' they could even constitute a crime against peace and eventually fall within the jurisdiction of the ICC.[70]

---

64 See Kastner and Mégret (Ch 12 of this Handbook).

65 See Roscini (Ch 14 of this Handbook).

66 See e.g., Yoram Dinstein, 'Computer network attacks and self-defense' (2001) 76 *Intl L Studies* 99, 103.

67 Christopher Joyner and Catherine Lotrionte, 'Information warfare as international coercion: Elements of a legal framework' (2001) 12 *EJIL* 825, 855.

68 *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion [1996] ICJ Rep 226, para 39.

69 Roscini (n 51) 106.

70 Ibid., 111–13. As is well known, jurisdiction over the crime of aggression, originally mentioned in Article 5 ICC Statute, was introduced at the 2010 Kampala Review Conference (see n 162 below). On 14 December 2017 the ICC Assembly of the States Parties decided by Resolution ICC-ASP/16/Res.5 to

(c) 'Armed Attack' for Self-defence Purposes

However, not any 'use of force' is an armed attack for self-defence purposes.[71] Under Article 51 only an 'armed attack' justifies self-defence,[72] but the term 'armed attack' is not defined by Article 51 or any other treaty rule.[73] While the term was probably considered 'self-evident' in 1945,[74] in the *Nicaragua Case* the ICJ noted that 'there appears now to be general agreement on the nature of the acts which can be treated as constituting armed attacks'.[75] Famously, the Court has distinguished 'the most grave forms of the use of force from other less grave forms',[76] holding that there are 'measures which do not constitute an armed attack but may nevertheless involve a use of force'. In the Court's view the supply of weapons and logistical support to rebels or 'a mere frontier incident' do not qualify as armed attacks under Article 51, although they are unlawful uses of force under Article 2(4).[77] In any event self-defence is permitted only when the armed attack exhibit certain 'scale and effects'.[78] By such standard, a cyber attack will constitute an 'armed attack' under Article 51 if its scale and effects meet the threshold corresponding to the 'most grave' forms of the 'use of force'.[79] The *Institut de Droit International* endorsed this view in its Santiago Resolution of 2007 on self-defence.[80]

---

activate the Court's jurisdiction over the crime of aggression as of 17 July 2018 https://asp.icc-cpi.int/iccdocs/asp_docs/Resolutions/ASP16/ICC-ASP-16-Res5-ENG.pdf accessed 7 February 2020.

71 Waxman (n 47) 421.

72 *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States)*, Judgment [2003] ICJ Rep 161, para 51.

73 *Nicaragua Case (Merits*) (n 1) para 176, 'a definition of the "armed attack" which, if found to exist, authorizes the exercise of the "inherent right" of self-defence, is not provided in the Charter, and is not part of treaty law'.

74 Ian Brownlie, *International Law and the Use of Force by States* (Clarendon Press 1963) 278.

75 *Nicaragua Case (Merits*) (n 1) para 195.

76 Ibid., paras 191, 210; *Oil Platforms* (n 72) paras 161, 186–7.

77 *Nicaragua Case (Merits*) (n 1) para 195.

78 Ibid., paras 191 and 195. For a comment on the terms 'scale' and 'effects' see Avra Constantinou, *The Right of Self-Defence under Customary International Law and Article 51 of the UN Charter* (Sakkoulas 2000) 63–4.

79 The former Legal Advisor US Department of State, Koh (n 54) stated in the specific context of cyber attacks that:

> the United States has for a long time taken the position that the inherent right of self-defense potentially applies against any illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an "armed attack" that may warrant a forcible response. But that is not to say that any illegal use of force triggers the right to use any and all force in response—such responses must still be *necessary* and of course *proportionate*..

However, the position of one State is irrelevant to general international law: see e.g., the 2006 *Jones* judgment by the UK House of Lords [2006] UKHL 26, para 22 ('one swallow does not make a rule of international law' *per* Lord Bingham of Cornhill), and the 2012 *Jurisdictional Immunities of the State (Germany v. Italy; Greece intervening)*, Judgment [2012] ICJ Rep 99, paras 83 and 88, both criticizing the (only) Italian jurisprudence favouring a 'humanitarian exception' to the jurisdictional immunity of foreign States accused of serious violations of human rights.

80 Institut de Droit International, 'Present Problems of the Use of Armed Force in International Law. A. Self-defence' (10A Resolution, Session de Santiago, 27 October 2007) para 5 http://www.idi-iil.org/app/uploads/2017/06/2007_san_02_en.pdf accessed 7 February 2020:

> An armed attack triggering the right of self-defence must be of a certain degree of gravity. Acts involving the use of force of lesser intensity may give rise to countermeasures in conformity with international law. In case of an attack of lesser intensity the target State may also take strictly

While the term 'use of force' in Article 2(4) is generally meant to include non-kinetic action, the term 'armed' in Article 51 may be understood as to imply the use of weapons. However, as hinted earlier, in the 1996 *Nuclear Weapons* Advisory Opinion the ICJ stated that Article 2(4), Article 51 and Article 42 UN Charter 'do not refer to specific weapons' and hence 'apply to any use of force, regardless of the weapons employed'. According to the Court '[t]he Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons'.[81]

The question then arises as to when a cyber attack amounts to an 'armed attack' and justifies self-defence. Cyber attacks conducted as part of an overall 'classic' military kinetic operation, such as attacks against enemy command and control or air defence systems, are subject to the international law rules (concerning the recourse to force and international humanitarian law) applicable to kinetic armed attacks.[82] As for standalone cyber attacks, many commentators agree that here again the effect- and target-based approaches to the interpretation of Article 51 should be adopted, although setting the bar higher: a cyber attack is held to amount to an 'armed attack' when it causes death or injury to persons or damage to property similar in scale and effects to kinetic attacks,[83] which may easily occur when the 'critical infrastructure' of the State (or other political entity such as the EU) is hit,[84] such as the shutdown of computers controlling waterworks and dams leading to the flooding of inhabited areas.[85] Rule 71 of the Tallinn Manual 2.0 adopts this approach.[86] Other kinds of attacks may not reach the threshold. It has been suggested, for example, that the mere destruction or damage of data, standing alone, would not suffice since, otherwise, the vast majority of cyber attacks would qualify as armed attacks and justify self-defence.[87] Moreover, an intention-based approach seems to have only a secondary relevance, what counts being objective effects, even on a third State which is not the intended target of the attack.[88] In *Oil Platforms* the ICJ specified that an armed attack has to be carried out 'with the specific intention of harming', although it is unclear whether the Court meant a general requirement for self-defence or merely referred to the instant case. Since cyber attacks may well hit third States, the Court's position seems to imply that States other than the intended target State may not respond in self-defence.[89]

Whether customary international law, in addition to Article 51 UN Charter, permits self-defence against cyber attacks is controversial. The question arises because international customary law still applies 'separately from international treaty law'.[90] Some scholars have

---

necessary police measures to repel the attack. It is understood that the Security Council may take [effective measures necessary to maintain or restore international peace and security].

81 See *Legality of the Threat or Use of Nuclear Weapons* (n 68).

82 Schmitt (n 3) 588.

83 For a number of hypothetical examples, see ibid.; Dinstein (n 66).

84 For the view that 'a cyber attack on critical state infrastructure which paralyses or massively disrupts the apparatus of the State should be equated to an armed attack, even if it does not cause any immediate human injury or material damage' see Tsagourias (n 45) 231.

85 Dinstein (n 66) 105; Yoram Dinstein, *War, Aggression and Self-Defence* (CUP 2017) 221.

86 Schmitt (n 18) rule 71.

87 Schmitt (n 3) 589.

88 Ibid., 590.

89 *Oil Platforms* (n 72) para 64.

90 *Nicaragua Case (Merits*) (n 1) para 179.

answered the question negatively.[91] Others have countered that even in the absence of actual practice *usus* is made up also of 'verbal acts' and 'is more a qualitative than a quantitative criterion', and in any event several States and, to use the ICJ's language,[92] 'specially affected' non-State entities (e.g., NATO) have taken a stance in favour of the right to self-defence against cyber attacks and triggered a process, which is ongoing, which may lead 'in the forthcoming years' to the formation of a customary rule.[93] The issue is, however, of little practical relevance since virtually all States are parties to the UN Charter and, as a specific consequence in relation to self-defence, it is difficult to imagine a real 'gap' between Article 51 and customary international law. A reaction by a non-State entity not being a party to the UN Charter, such as NATO, would very likely be seen as a reaction of its member States in the form of collective self-defence under Article 5 of the NATO Treaty.[94]

(d) 'Critical Infrastructure' Targeted by Cyber Attacks[95]

The notion of 'critical infrastructure' is relatively novel and difficult to define.[96] It has to do, inter alia, with 'national security' but not any threat to the national security of a State justifies a response in self-defence and the notion of 'national security' itself is unclear.[97] Moreover, the notion of 'critical infrastructure' varies in time and space. It also depends on the very process of State informationalization since what was not seen as 'critical' in the past or under other circumstances may become 'critical' as a result of the State informationalization process itself.[98] To complicate matters, in most States critical infrastructures are often owned by the private sector.[99]

Broadly speaking, critical infrastructure is defined as the assets that are essential for the functioning of a society and economy, notably for the supply of essential services. It refers to such infrastructures as power plants, water systems, dams, gas pipelines, chemical plants and reactors, transports (airlines, ferries, railways, highways, etc.), energy networks for production, transport and distribution (such as gas pipelines, gas storage facilities, electric trunks, electric transformers, energy generation plants and fuel distribution), financial and bank net-

---

[91] See e.g., Schmitt (n 53) 921 ('Neither practice, nor *opinio juris*, is in evidence'); Shackelford (n 56) 219 ('it is yet impossible as a matter of customary international law to argue that IW is illegal, especially given that state practice routinely shows otherwise').

[92] *North Sea Continental Shelf (Federal Republic of Germany v. Denmark and Federal Republic of Germany v. Netherlands)*, Judgment (Merits) [1969] ICJ Rep 4, para 73.

[93] Roscini (n 51) 123–30.

[94] See n 32.

[95] See also Roscini (Ch 14 of this Handbook).

[96] Eric T Jensen, 'Computer attacks on critical national infrastructure: A use of force invoking the right to self-defense' (2002) 38 *Stanford J of Intl L* 207.

[97] Theodore Christakis, 'L'Etat avant le droit? L'exception de "sécurité nationale" en droit international' (2008) 112 *Revue Générale de Droit International Public* 5, 8–16.

[98] UNGA Res 58/199 (23 December 2003) UN Doc A/RES/58/199 recognizes that 'each country will determine its own critical information infrastructures' defined as 'such as those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health—and the critical information infrastructures that increasingly interconnect and affect their operations'; see also UNGA Res 64/211 (21 December 2009) on the 'Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures'.

[99] Roscini (n 51) 118.

works, water and food distribution, ICT networks such as Internet (both its physical and virtual infrastructure), radio, TV networks, cabled broadcast and satellite communications, the health system, government and military networks and emergency networks.

For example, EU Council Directive 2008/114/EC of 8 December 2008[100] establishes a procedure for the identification and designation of European critical infrastructures ('ECIs') and a common approach to the assessment of the need to improve their protection (Art 1), defines 'critical infrastructure' as 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions' (Art 2(a)). This definition has been reiterated in Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems.[101]

The US 'Patriot Act of 2001' defined critical infrastructure as those 'systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters'.[102] It has been suggested that a cyber attack against a State's military assets and capability amounts to an armed attack for self-defence purposes[103] and that:

> cyber attacks on the controlling information technology for a nation's infrastructure that had a significant impact on the functioning of that infrastructure (whether or not it caused immediate large-scale death or destruction of property) would be an armed attack for Article 51 purposes, just as would a kinetic attack that somehow managed to shut down the system without such immediate secondary effects.[104]

Others have replied that much depends on the effects of the attack and the military character of the target is hardly relevant;[105] moreover, although this may be the case in State practice, it

---

[100] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ L 345/75). On 23 July 2019 the EU Commission released a report finding that some of the definitions contained in the 2008 Directive were too broad and that the Directive is only of partial relevance today, https://ec.europa.eu/home-affairs/news/commission-evaluates-implementation-directive-protecting-european-critical-infrastructures_en accessed 7 February 2020.

[101] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L 218/8.

[102] Section 1016 (e) of *Public Law 107-56* of 26 October 2001, 'The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001' commonly known as the 'USA Patriot Act' http://epic.org/privacy/terrorism/hr3162.pdf accessed 7 February 2020.

[103] Herbert S Lin, Kenneth W Dam and William A Owens (eds), *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (National Academies Press 2009) 245, 'cyber attacks that compromise the ability of units of the DOD to perform the DOD's mission might well be regarded as an armed attack, and indeed STRATCOM has the authority to conduct response actions to neutralize such threats'.

[104] Ibid., 254.

[105] Schmitt (n 3) 589.

is not law as it stands.[106] The same definition has been used by Executive Order No 13636 of 12 February 2013, 'Improving Critical Infrastructure Cybersecurity'.[107]

Unsurprisingly NATO also considered its own 'contribution to meet security challenges to critical infrastructure', assuming that '[t]he impact of attacks against critical infrastructure can be devastating to the livelihoods of modern societies' and '[t]he increasing reliance on complex and networked technology and access to global markets make our societies highly vulnerable to disruptions'.[108]

6. ANTICIPATORY SELF-DEFENCE[109]

Is anticipatory self-defence permitted against a mere threat of cyber attack or against an attack which does not reach the threshold of an 'armed attack'? The question is highly debated and the ICJ abstained from pronouncing on it in the *Nicaragua Case*.[110] In *Armed activities in Congo* the Court opined that 'Article 51 of the Charter may justify a use of force in self-defence only within the strict confines there laid down' and 'does not allow the use of force by a State to protect perceived security interests beyond these parameters'.[111] A few States accept that anticipatory self-defence is permitted, arguing that technological advances in weapons make anticipatory self-defence a matter of necessity, whatever the language of Article 51. Most States, however, seem to take the opposite stand, believing that a broad notion of anticipatory self-defence based on remote attacks shades off into a justification of aggression, which is unquestionably prohibited. In its 2007 Resolution on self-defence the *Institut de Droit International* stated that: 'The right of self-defence arises for the target State in case of an actual or manifestly imminent armed attack', there being 'no basis in international law for the doctrines of "preventive" self-defence in the absence of an actual or manifestly imminent armed attack'.[112] The *Institut* thus seems to accept anticipatory self-defence in case it is necessary to face a 'manifestly imminent'—hence, impliedly, not merely hypothetical or

---

[106] Ibid., 604.

[107] White House, 'Improving Critical Infrastructure Cybersecurity' (Executive Order No 13636 of 12 February 2013) https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity accessed 7 February 2020.

[108] See NATO Emerging Security Challenges Division, '*The World in 2020 – Can NATO Protect Us? The Challenges to Critical Infrastructure*' (Conference Report 10 December 2012, Brussels) http://natolibguides.info/ld.php?content_id=1675627,
accessed 7 February 2020.

[109] The terminology on self-defence against 'threats' rather than (ongoing or already occurred) attacks is anything but univocal. Different terms are often used and even identical terms may have different meanings in different authors and in international practice depending, inter alia, on the nature, level or imminence of the threat. In this chapter the term 'anticipatory self-defence' is used as an umbrella term whereas other terms, such as 'pre-emptive' 'preventive' and 'interceptive' self-defence, will be referred to below with the meanings attached to them by specific authors or in specific contexts.

[110] *Nicaragua Case (Merits)* (n 1) para 194:
> reliance is placed by the Parties only on the right of self-defence in the case of an armed attack which has already occurred, and the issue of the lawfulness of a response to the imminent threat of armed attack has not been raised. Accordingly the Court expresses no view on that issue.

[111] *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgment [2005] ICJ Rep 168, paras 143 and 148.

[112] Institut de Droit International (n 80) paras 3 and 6.

remote— armed attack. This is a reasonable position and is shared by the UN legal doctrine,[113] although the Non-Aligned Movement (NAM) appears firmly against any form of anticipatory self-defence.[114]

Article 51, when read literally, seems to require that an attack is underway. As is well known, the literature is divided. Some argue that self-defence is permitted when faced with an 'imminent' threat, relying on US Secretary of State Webster's famous statement of 1841 in *Caroline*, which was affirmed by the Nuremberg Tribunal,[115] whereby the necessity for self-defence must be 'instant, overwhelming, leaving no choice of means, and no moment of deliberation'.[116] Others argue that Article 51 prohibits anticipatory self-defence.[117] Still others have introduced a middle-path notion of 'interceptive' self-defence, i.e., a reaction to an attack already launched and about to strike the target even if the target has not yet been hit.[118] The 2002 'Bush Doctrine', reaffirmed by the US in its '2006 National Security Strategy', admitted anticipatory self-defence in very broad terms, i.e., even when the threat is not imminent but possible or merely prospective and linked it with the military reaction to the 'war on terror'.[119] The 2010 National Security Strategy by US President Obama did not mention pre-emption although it did not reject it either and reserved the right of the US to act unilaterally if necessary.[120] On 11 January 2017 the UK Attorney General Jeremy Wright, in a speech on 'The Modern Law of Self-Defence' held, in summary, that the use of force in self-defence against an imminent attack is allowed, although '[i]t is absolutely not the position of the UK Government that armed force may be used to prevent a threat from materialising in the first place'. In a speech made on 'The Right of Self-Defence Against Imminent Armed Attack in International Law' on 11 April 2017 the Australian Attorney General George Brandis proceeded along similar lines.[121]

In the 1996 *Nuclear Weapons* Advisory Opinion the ICJ, noting 'the fundamental right of every State to survival, and thus its right to resort to self-defence, in accordance with Article 51 of the Charter, when its survival is at stake', observed that 'it cannot reach a definitive

---

[113] E.g., in its 2004 'a more secure world: Our shared responsibility' Report the UN-mandated High-Level Panel on Threats, Challenges and Change distinguished between lawful 'pre-emptive' self-defence when the attack is imminent, and unlawful (unless authorized by the Security Council) 'preventive' self-defence when the alleged attack is too remote (UN Doc A/59/565 paras 188–92). This opinion has apparently been endorsed by the UN Secretary-General in his 'In larger freedom: Towards development, security and human rights for all' (Report, 21 March 2005) UN Doc A/59/2005 para 124.

[114] UNGA, 'NAM Comments on the High-level Panel Report' (28 February 2005) UN Doc A/59/PV, 43 http://www.un.int/malaysia/NAM/Positionpaper280205.doc accessed 25 February 2014.

[115] *Trial of the Major War Criminals* (Judgment) [1946] (1947) 41 *AJIL* 172, 205.

[116] John B Moore, *A Digest of International Law* (Government Printing Office 1906) vol 2, 409–10.

[117] E.g., according to Christine D Gray, *International Law and the Use of Force* (OUP 2008) 165 and 213 '[t]here is very little international support for this [Bush] doctrine of pre-emptive self-defence'.

[118] Dinstein, *War, Aggression and Self-Defence* (n 85) 231–3.

[119] See Christine D Gray, 'The Bush doctrine revisited: The 2006 National Security Strategy of the USA' (2006) 5 *Chinese J of Intl L* 555.

[120] White House, 'National Security Strategy' (May 2010) http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf accessed 3 September 2014.

[121] UK Attorney General, 'The Modern Law of Self-Defence', 11 January 2017, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/583171/170111_Imminence_Speech_.pdf; Australian Attorney General, 'The Right of Self-Defence Against Imminent Armed Attack in International Law' (25 May 2017) EJIL: *Talk!*, https://www.ejiltalk.org/the-right-of-self-defence-against-imminent-armed-attack-in-international-law/.

conclusion as to the legality or illegality of the use of nuclear weapons by a State in an extreme circumstance of self-defence, in which its very survival would be at stake'.[122] It is a fact, however, that Article 51 refers to the condition that 'an armed attack occurs' and it is the provision thus formulated that binds member States. The term 'inherent', far from indicating that Article 51 resumed the pre-Charter rule on permissibility of anticipatory self-defence,[123] simply seem to take note that self-defence reflects the universal principle *vim vi repellere licet*. In the 1981 *Osirak* incident, many States condemned anticipatory self-defence,[124] and they have eventually continued to do so on other occasions. In the 2004 report *A More Secure World* the UN-mandated High-Level Panel distinguished between lawful 'pre-emptive' self-defence when the attack is imminent, and unlawful (unless authorized by the Security Council) 'preventive' self-defence when the alleged attack is too remote,[125] an opinion which has apparently been endorsed by the UN Secretary-General[126] but opposed by the Non-Aligned Movement (NAM).[127]

Article 51 and its expression 'if an armed attack occurs' remain, even under the terms of the ICJ *Nuclear Weapon* Opinion, the basic parameter. On balance, it seems that the international community does not accept anticipatory self-defence *as a general rule*, but could see it as a justification on a case-by-case basis. The general rule is thus that anticipatory self-defence is prohibited and that its permissibility depends on the reaction of the international community as a whole in each case. Any attempt to articulate the law further goes too far. Thus understood, anticipatory self-defence is not permitted under Article 51, which has to be read literally, and rather overlaps with the state of necessity in general international law as a justification for an otherwise unlawful use of force.[128] Not surprisingly preventive self-defence was permitted and closely linked to self-preservation in the nineteenth century when recourse to force in general was, unlike today, permitted. It may be condoned *ex post* by the international community on a case-by-case basis if the threat to the State proves well-founded on the basis of the knowledge and inferences which can be drawn at the moment of deliberation. In any event, Article 51 applies and justifies 'interceptive' self-defence,[129] while military intervention against a 'threat to peace' authorized by the UN Security Council, when this is permitted, is justified under Chapter VII.

Concerning the threats of cyber attack, the *Caroline* criteria are thought by some to be still valid and to apply.[130] It has been suggested that anticipatory self-defence is 'a reasonable

---

[122] *Legality of the Threat or Use of Nuclear Weapons* (n 68) para 97.

[123] Derek W Bowett, *Self-Defense in International Law* (Praeger 1958) 188–92. Against this view see *Brownlie* (n 74) 428–36.

[124] UN Doc SCOR, 36th year, 2280th–2283rd, 2286th and 2288th meetings, and UNSC Res 487 (1981) (19 June 1981) adopted unanimously, condemning the attack.

[125] UNGA 'Note by the Secretary-General' (2 December 2004, 'A more secure world: Our shared responsibility, Report of the High-Level Panel on Threats, Challenges and Change') UN Doc A/59/565 paras 188–92.

[126] UNSG, 'In Larger Freedom (n 113) para 124.

[127] See 'Comments' (n 114).

[128] Cf. Art 25 UN 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries' (2001) GAOR 56th Session Supp 10, 43. For some further observations on the point see Carlo Focarelli, *International Law as Social Construct: The Struggle for Global Justice* (OUP 2012) 367–8.

[129] See Dinstein, *War, Aggression and Self-Defence* (n 85).

[130] Schmitt (n 53) 932–3.

accommodation' to present circumstances permitted when an 'overtly hostile intent' to launch a cyber attack exists together with a decision to attack and the planned attack is likely to generate armed attack consequences.[131] In particular, anticipatory self-defence is permitted if the prospective attack: (a) is part of an overall operation culminating in armed attack; (b) is an irrevocable step in an imminent and probably unavoidable attack; and (c) the response is a last resort measure to effectively counter the attack.[132] This position sounds sensible on the one hand, but, on the other and at the same time, quite artificial. It is sensible because, given the speed of electronic operations and their possible immediate devastating effects, only anticipatory self-defence makes sense and leaves the attacked State an effective possibility of defending itself. But it is also artificial, or purely speculative, because cyber attacks are extremely difficult to trace even *after* their occurrence and it is difficult to see how the target State may take action without hitting arbitrarily the supposed potential source of attack.

7. CONDITIONS CONCOMITANT TO THE EXERCISE OF SELF-DEFENCE

Self-defence has to be carried out by complying with necessity and proportionality, as the ICJ stated in the *Nicaragua Case*[133] and in *Oil Platforms*,[134] with Rule 72 of the Tallinn Manual 2.0 affirming such requirements.[135] The threshold may suffer from some alteration as a result of the unique features of cyber attacks.

Necessity requires that no other reasonable option is available other than force (such as non-forcible measures or cyber defences) to effectively repel the attack, or to deter a threat of (an imminent) attack if anticipatory self-defence is accepted. For example, if passive cyber defences are sufficient to repel an ongoing attack (or to deter a prospective attack) forceful measures are not necessary.[136] This implies that *States have an obligation to put in place passive or active cyber defences* (not amounting to a prohibited use of force[137]) in order to block electronically cyber attacks and thus prove that such defences are insufficient to attain the aim of self-defence. For example, the *World in 2020* NATO report stated that 'Over time, NATO should plan to mount a fully adequate array of cyber defence capabilities, including passive and active elements.'[138] It is worth noting that necessity applies to both kinetic and cyber counter-attacks in self-defence. In particular, cyber self-defence causing harm similar to kinetic (forceful) self-defence is permitted only when lesser cyber counter-attacks reasonably capable of repelling the attack (or deterring an imminent attack if anticipatory defence is accepted) are unavailable.

---

131 Schmitt (n 3) 592–3.
132 Schmitt (n 53) 932–3.
133 *Nicaragua Case (Merits*) (n 1) para 194.
134 *Oil Platforms* (n 72) paras 161, 183, 196–8.
135 Schmitt (n 18) rule 72.
136 In principle 'passive' cyber defences such as firewalls and antivirus software, which merely block attacks are internationally lawful acts, although they may amount to a violation of an international law rule other than that prohibiting the use of force.
137 Schmitt (n 3) 586.
138 NATO Emerging Security Challenges Division (n 108) 45.

Proportionality requires that, once force is deemed to be necessary, the amount of force used does not exceed what is sufficient to repel or, if anticipatory self-defence is accepted, to deter the threat of attack. A few States and some commentators have relied on the 'accumulation of events' or 'pin prick' doctrine of armed attack so as to justify an otherwise disproportionate response. In the *Nicaragua Case* the ICJ seems not to dismiss this doctrine,[139] but avoided explicitly discussing the point in subsequent cases either.[140] It is worth noting that, just like necessity, proportionality applies to both kinetic and cyber counter-attacks in self-defence. Cyber self-defence causing harm similar to kinetic (forceful) self-defence is thus permitted only when a smaller amount of force is insufficient to repel the attack (or to deter an imminent attack). Of course, cyber self-defence may prove inherently inadequate so that recourse to kinetic self-defence is not only necessary but also proportionate, provided it is scaled to the purpose of repelling or, if anticipatory self-defence is accepted, deterring the threat of attack. It is often believed that a response in kind is inherently proportionate but this depends on the notion of proportion accepted: for example, if proportion refers to the harm suffered it may well be that the same action causes very different levels of harm in different States.[141] As a result proportionality applies also to reactions in kind. The application of the 'accumulation of events' to cyber operations is rather controversial.[142]

Immediacy seems more a necessity than a requirement in a cyber context, where speed is key. It is commonly accepted that immediacy has to be understood flexibly. This applies a fortiori in a cyber context when considering that it may take a long time to trace the attack back to its originator or for damage to occur after the attack. Rule 73 of the Tallinn Manual 2.0 sets out such a requirement.[143]

8. COLLECTIVE SELF-DEFENCE

Article 51 permits collective self-defence in addition to individual self-defence, i.e., armed action against an armed attack by a State other than the attacked State. The possibility of col-

---

[139] *Nicaragua Case (Merits*) (n 1) para 231.

[140] Gray (n 119) 155–6; Dinstein, *War, Aggression and Self-Defence* (n 85) 211–3.

[141] See e.g., Dapo Akande and Thomas Liefländer, 'Clarifying necessity, imminence, and proportionality in the law of self-defense' (2013) 107 *AJIL* 563, 566–8, distinguishing three conceptions of proportionality 'each ha[ving] different implications' (no more force than necessary, commensurability with the attack or the threatened attack, damage inflicted proportionate to the pursued objective). It is worth noting that similar problems exist with non-forcible countermeasures. In the 1978 *Air Services* Award the Arbitral Tribunal articulated the condition of proportionality by observing that countermeasures must have 'some degree of equivalence with the alleged breach' this being 'a well-known rule' which both Parties had recognized and invoked in the instant case; however, in the Tribunal's view, 'judging the "proportionality" of countermeasures is not an easy task and can at best be accomplished by approximation' taking into account 'not only the injuries suffered by the companies concerned but also the importance of the questions of principle arising from the alleged breach' (cf. *Case concerning the Air Service Agreement of 27 March 1946 between the United States and France* (Award) [1978] 18 *Reports of International Arbitral Awards* 417 para 83). What was meant by 'questions of principle' is unclear; still, the Tribunal's view was unquestionably that damages alone were inadequate for an accurate assessment of proportionality. See further on this Focarelli (n 128) 351–2.

[142] Roscini (n 51) 120.

[143] Schmitt (n 18) rule 73.

lective self-defence may be stipulated in a military alliance treaty, as is the case with Article 5 of the NATO Treaty,[144] or more generally in bilateral and multilateral mutual assistance treaties. However, as the 'NATO 2020' report pointed out, 'there may well be doubts about whether an unconventional danger—such as a cyber attack or evidence that terrorists are planning a strike—triggers the collective defence mechanisms of Article 5'.[145] And yet 'the risk of a large-scale attack on NATO's command and control systems or energy grids could readily warrant consultations under Article 4 and could possibly lead to collective defence measures under Article 5'.[146] Rule 74 of the Tallinn Manual 2.0 adopts this approach.[147]

Self-defence in general, including collective self-defence, may be resorted to unilaterally, without any authorization of the Security Council, although it must cease if and when the Council takes action. However, it is permitted only—in addition to the requirements of necessity, proportionality and immediacy—on the basis of a request by (and hence with and within the consent of) the attacked State, as the ICJ specified in the *Nicaragua Case*[148] and in *Oil Platforms*.[149] In other words, it is not for third States to determine whether another State has been the victim of an armed attack. Should the response not conform to such a requirement, the counter-attack by a third State is an unlawful use of force.

Cyber attacks may easily spread through networks and it may be difficult to identify the 'attacked' State which has the right to consent to a counter-attack. Many States may well be considered attacked and entitled to react in *individual* self-defence. It is also necessary that all member States of a mutual assistance treaty agree on considering a certain cyber attack as an attack justifying collective reaction. Moreover, treaty provisions on collective self-defence generally entitle all member States to react but do not provide an obligation to do so and it is therefore reasonable to expect that they take part in the collective response only when it fits with their national interest. For instance, in the case of Estonia NATO member States were very slow to agree on responding in self-defence.[150]

9. SELF-DEFENCE AGAINST NON-STATE ACTORS

The question whether non-State actors may carry out an 'armed attack' under Article 51 is heatedly debated.[151] Self-defence has been traditionally understood as a *State* reaction against another *State*. The ICJ seems to have endorsed the view that self-defence is an inter-State

---

[144] See n 32.

[145] 'NATO 2020: Assured Security, Dynamic Engagement. Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO' (17 May 2010) 20 www.nato.int/strategic-concept/expertsreport.pdf accessed 30 November 2013.

[146] Ibid., 45.

[147] Schmitt (n 18) rule 74.

[148] *Nicaragua Case (Merits*) (n 1) para 199.

[149] *Oil Platforms* (n 72) para 188.

[150] Schmitt (n 3) 598.

[151] Noam Lubell, *Extraterritorial Use of Force against Non-State Actors* (OUP 2010); Theresa Reinold, 'State weakness, irregular warfare, and the right to self-defense post-9/11' (2011) 105 *AJIL* 244; Mary Ellen O'Connell, Christian J Tams and Dire Tladi (eds), *Self-Defence against Non-State Actors* (CUP 2019).

measure,[152] although some of its judges have argued for the admissibility of 'self-defence against non-state actors'.[153] However, Article 2(4) specifies that the 'use of force' prohibited has to come from a State and an 'armed attack' under Article 51 is a per se prohibited 'use of force' in the first place. Unlawful acts by private individuals or groups in principle fall within the criminal law of the territorial State and the international law rules concerning the allocation of criminal jurisdiction, criminal mutual assistance (including extradition) and, in extreme cases, national and international prosecution of international crimes according to the 'law-enforcement' paradigm. It is in principle for the State to prevent transnational crime and to punish perpetrators.

However, certain States in the territory of which harm was caused by criminal acts committed by private individuals or groups (rebels or alleged terrorists) from another State have invoked self-defence even in cases where such criminal acts were not attributable to this latter State. On the occasion of the War on Afghanistan in 2001 most States, the UN Security Council and other international organizations apparently endorsed the view that self-defence was permitted against Afghanistan regardless of the attacks suffered being performed on behalf of the State of Afghanistan. In relation to the Israeli-Lebanese War in 2006 most States apparently accepted Israel's contention that self-defence against Hezbollah was permitted, at least when the territorial State (like Lebanon in that case) proves unable to prevent the attacks and even asks for assistance from the international community, although many States and commentators pointed out that the reaction was out of proportion to the extent that Israel targeted Beirut and Lebanese areas other than those from which the attack had been launched.[154] There is in legal doctrine some support for self-defence against non-State actors accompanied by a trend by its advocates to regard its critics (as well as the ICJ's jurisprudence on the matter) as 'conservative'.[155] Another similar trend consists in admitting self-defence against non-State actors as a corollary of the responsibility to protect doctrine specifically understood as a 'duty to prevent'.[156] In its 2007 Resolution on self-defence the *Institut de Droit International* stated that 'Article 51 of the Charter as supplemented by customary international law applies as a matter of principle' and provided only 'some preliminary responses to the complex problems' arising out of the matter, concluding that 'The State from which the armed attack by non-State actors is launched has the obligation to cooperate with the target State'.[157]

The debate raged when in Resolution 1368 (2001) and in Resolution 1373 (2001) the UN Security Council affirmed the inherent right to self-defence without specifying whether the source of the armed attack had to be a State, apparently suggesting that the attribution requirement and the concomitant acceptance of the concept of a 'private' armed attack could

---

[152] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion [2004] ICJ Rep 136, para 139; *Armed Activities on the Territory of the Democratic Republic of the Congo v. Uganda* (n 111) para 160.

[153] *Legal Consequences of the Construction of a Wall* (n 152) para 139.

[154] Cf UN Doc S/PV.5489 of 14 July 2006 and S/PV.5492 of 20 July 2006. See Gray (n 117) 241–4; more generally, see Jörg Kammerhofer, 'The armed activities case and non-state actors in self-defence law' (2007) 20 *Leiden J of Intl L* 89.

[155] Reinold (n 151) 245, 260, 262 and 285.

[156] Lee Feinstein and Anne-Marie Slaughter, 'A duty to prevent' (2004) 83 *Foreign Affairs* 136. See generally Carlo Focarelli, 'Responsibility to Protect in the Global System' in Peter Hilpold (ed), *Responsibility to Protect (R2P): A New Paradigm of International Law?* (Brill 2015) 417–38.

[157] Institut de Droit International (n 80) para 10.

be abandoned.[158] There are clear signs of possible abuse and likely divergence of views among States. For example, according to the Russian Federation, Resolution 1373 (2001) also covers Chechen rebels and justifies self-defence against States (such as Georgia) from the territory of which they launch their attacks.[159] Not surprisingly, the Russian appeal to the doctrine of self-defence against non-State actors was immediately opposed by one of its stronger advocates, the US, each, of course, being concerned with their own private 'enemies'.[160] In fact, cross-border military incursions against alleged terrorists operating in neighbouring States are generally condemned assuming that the crimes committed by the targeted individuals and groups fall within the law enforcement paradigm and do not justify self-defence against the territorial State. For example, a Colombian raid against the FARC in the territory of Ecuador, in 2008, was condemned in the OAS Permanent Council by Resolution 930 (2008).[161] Furthermore, the definition of the crime of aggression adopted at the 2010 Review Conference of the ICC Statute of Kampala does not mention the harbouring of irregular forces. It only includes, by mirroring UN General Assembly Resolution 3314 (XXIX) of 14 December 1974 and in line with the ICJ *Nicaragua Case* Judgment, the active sending of armed bands by, or on behalf of, a State to carry out acts of armed force against another State.[162]

Furthermore, attribution is very relevant here. In theory, a 'non-State' actor is by definition an entity which acts privately with no connection at all with a State.[163] However, 'sponsorship' by a State is frequently invoked as a characteristic of 'self-defence against non-state actors'. On attribution, and more precisely on 'control' as an attribution criterion, it is well known that

---

[158] See e.g., Thomas M Franck, 'Terrorism and the *right* of self-defense' (2001) 95 *AJIL* 839, 840; Christopher Greenwood, 'International law and the pre-emptive use of force: Afghanistan, Al-Qaida, and Iraq' (2003) 4 *San Diego Intl L J* 7, 17.

[159] The Russian Federation accused Georgia of failure to comply with UNSC Res 1373 (28 September 2001) UN Doc S/RES/1373, pointing out that such failure justified self-defence under art 51 UN Charter. According to Russia:

> If the Georgian leadership is unable to establish a security zone in the area of the Georgian-Russian border, continues to ignore UNSC Res 1373 (28 September 2001) and does not put an end to the bandit sorties and attacks on adjoining areas in the Russian Federation, we reserve the right to act in accordance with Article 51 of the Charter of the United Nations.

Cf. Statement by Russian Federation President Vladimir Putin, 'Annex to Letter dated 11 September 2002 from the Permanent Representative of the Russian Federation to the United Nations Addressed to the Secretary-General' UN Doc S/2002/1012, 2–3.

[160] Steven L Myers, 'Echoing Bush, Putin asks U.N. to back Georgia attack', *New York Times* (12 September 2002) A9; 'US warns Russia over Georgia strike', *BBC News* (13 September 2002) http://news.bbc.co.uk/2/hi/world/europe/2254959.stm accessed 7 February 2020.

[161] OAS Permanent Council Res 930 of 6 March 2008 http://www.oas.org/consejo/resolutions/res930.asp accessed 7 February 2020.

[162] ICC Res RC/Res 6 (11 June 2010) annex I, art 8*bis* (1) and (2) https://asp.icc-cpi.int/iccdocs/asp_docs/Resolutions/RC-Res.6-ENG.pdf. As to immediate comments, see Kai Ambos, 'The crime of aggression after Kampala' (2011) 53 *German Ybk of Intl L* 463; Stefan Barriga and Leena Grover, 'A historic breakthrough on the crime of aggression' (2011) 105 *AJIL* 517. For recent developments, see n 71.

[163] On attribution in cyber self-defence see Tsagourias (n 45) 233–43; for the international evidentiary standard to be applied, see O'Connell (n 4) 202; see also, most recently, Delerue (n 4); Henning Lahmann, 'Mistake of Fact in Putative Self-Defence Against Cyber Attacks' (17 January 2020) EJIL: *Talk!*, https://www.ejiltalk.org/mistake-of-fact-in-putative-self-defence-against-cyber-attacks/; Henning Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (CUP 2020).

the ICJ and the ILC on the one hand, and the ICTY on the other, has taken different views albeit in different legal contexts.[164] Attribution may actually take several different forms and degrees of State involvement, such as tolerance, causality, complicity, etc.[165] This ambiguity tends to make the issue overlap with that of self-defence against a failure of the State to prevent cross-border harmful action by private individuals or groups allegedly amounting to an 'armed attack' for self-defence purposes.[166]

There is no doubt that the duty of prevention of private cross-border harmful action is established in general international law. As famously held in the 1941 *Trail Smelter* Award 'under the principles of international law … no State has the right to use or permit the use of its territory in such a manner as to cause injury … in or to the territory of another or the properties or persons therein'.[167] Similar dicta had already been made, in relation to the utilization of international watercourses, by an Arbitral Tribunal in the 1928 *Island of Palmas* Award[168] and by the PCIJ in the 1929 *Oder River Commission* Judgment.[169] The principle was later restated by the ICJ in general terms in the 1949 *Corfu Channel* Judgment in terms of 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States',[170] and, specifically referring to environmental protection, in the 1996 *Nuclear*

---

[164] *Prosecutor v. Dusko Tadić* (Appeal Judgment of 15 July 1999) [1999] Case No ICTY-94-1-A paras 99–145; *Nicaragua Case (Merits*) (n 1) para 115; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment [2007] ICJ Rep 43, paras 403–7.

[165] The question about the criteria for attributing acts of non-State actors to a State in a State-orientated interpretation of self-defence have been developed, inter alia, by Elizabeth Wilmshurst, 'The Chatham House Principles of International Law on the use of force in self-defence' (2006) 55 *Intl and Comparative L Quarterly* 963–72; Daniel Bethlehem, 'Self-defense against an imminent or actual armed attack by nonstate actors' (2012) 106 *AJIL* 769. In our view these suggestions are no doubt interesting intellectual exercises but of little relevance (if not occasionally in fact campaigning for the stronger States) when it comes to establishing existing law. For some sharable critical comments, see Michael J Glennon, 'Law, power, and principles' (2013) 107 *AJIL* 378 ('Bethlehem's proposed principles … substitute the *opinio juris* of the powerful for the practice of all'); Mary Ellen O'Connell, 'Dangerous departures' (2013) 107 *AJIL* 380 ('Bethlehem offers to rewrite the rules, legalizing practices that today are violations of international law'); Gabor Rona and Raha Wala, 'No thank you to a radical rewrite of the *jus ad bellum*' (2013) 107 *AJIL* 387 ('Bethlehem's proposed principles … would reverse more than a century of humanitarian and human rights progress'); Dire Tladi, 'The nonconsenting innocent state: The problem with Bethlehem's principle 12' (2013) 107 *AJIL* 570, 576 (Bethlehem's 'principle 12 [admitting in certain circumstances the armed reaction against a state without its consent] is based on an erroneous assessment of customary international law and state practice and on an acontextual interpretation of Article 51').

[166] Roscini (n 51) 102.

[167] *Trail Smelter Case (United States v. Canada)* (Award) [1941] United Nations Reports of International Arbitral Awards (2006) 1905, 1965 http://legal.un.org/riaa/cases/vol_III/1905-1982.pdf accessed 7 February 2020.

[168] *Island of Palmas Case (Netherlands v. United States)* (Award) [1928] United Nations Reports of International Arbitral Awards (2006) 829, 839 http://legal.un.org/riaa/cases/vol_II/829-871.pdf accessed 7 February 2020.

[169] *Territorial Jurisdiction of the International Commission of the River Oder* (Judgment) [1929] PCIJ Ser A No 23 27.

[170] *Corfu Channel (United Kingdom v. Albania)*, Judgment (Merits) [1949] ICJ Rep 4, 22.

Weapons Advisory Opinion,[171] in the 1997 *Gabčíkovo-Nagymaros* Judgment,[172] in the 2010 *Pulp Mills* Judgment,[173] and in the 2015 *Border Area* Judgment,[174] as well as in Article 3 of the 1992 Biodiversity Convention.[175] The principle has been also thoroughly analysed by the ILC special rapporteur on natural disasters.[176] Briefly, a State's failure to prevent private actors on its territory from causing damage in the territory of another State constitutes an internationally unlawful act. Non-forcible countermeasures are thus permitted. The point is whether such a failure amounts to an 'armed attack' under Article 51, assuming that it would be so if directly carried out by (or if attributable to) a State, or in any case if it constitutes an international unlawful act of the State justifying self-defence.[177]

Self-defence against a State's failure to prevent private trans-border harm is distinct from self-defence against non-State actors is generally understood. The former is directed against a State's unlawful act, deriving from *its* failure to prevent private individuals and groups from causing cross-border harm through an action that if carried out by a State would amount to an 'armed attack' for self-defence purposes; while the latter appears as directed against the allegedly responsible individuals and groups as a response to *their* action and regardless of any attribution of *their* conduct to the State from the territory of which harm has been caused.

It has been argued that in the cyber context States would be willing to apply the same standard as in the terrorism context.[178] One might contend that in cyberspace the need for self-defence against non-State actors, however theorized, is particularly compelling. But if this view is accepted then what is talked about is an *autonomous* rule applying in cyberspace, a rule which, however, has little if any basis in existing international law and is thus only *promoted*, since the data and practice available concerning physical space are contentious at best. In UN General Assembly Resolution 55/63 of 4 December 2000 States are called upon to 'ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies', with no reference to self-defence or means other than those falling within the law enforcement paradigm.[179] It is a fact that 'substitutive' or 'extra-territorial' law enforce-

---

[171] *Legality of the Threat or Use of Nuclear Weapons* (n 68) para 29, ruling that the principle 'is now part of the corpus of international law relating to the environment'.

[172] *Gabčíkovo-Nagymaros Project (Hungary/Slovakia)*, Judgment [1997] ICJ Rep 7, paras 53 and 140.

[173] *Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Judgment [2010] ICJ Rep 14, para 101, holding that 'the principle of prevention, as a customary rule, has its origins in the due diligence that is required of a State in its territory' and reiterating what the Court had already stated in the 2006 Order (*Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Provisional Measures Order [2006] ICJ Rep para 72).

[174] *Certain Activities carried out by Nicaragua in the Border Area (Costa Rica v. Nicaragua)* and *Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica)*, Judgment [2015] ICJ Rep 665, para 104.

[175] Convention on Biological Diversity (concluded 5 June 1992, entered into force 29 December 1993) 1760 UNTS 79.

[176] See Carlo Focarelli, 'Duty to protect in cases of natural disasters' in Rüdiger Wolfrum (ed), *Max Planck Encyclopaedia of Public International Law* (OUP 2012).

[177] See Mahmoud Hmoud, 'Are new principles really needed? The potential of the established distinction between responsibility for attacks by nonstate actors and the law of self-defense' (2013) 107 *AJIL* 576, 577–8.

[178] Schmitt (n 3) 598–603.

[179] UNGA Res 55/63 (4 December 2000) para 1, on 'Combating the criminal misuse of information technologies'.

ment by other States is rooted in an imperial global order with the stronger States (never the weaker ones for obvious reasons) operating as the 'international police', inevitably to further their particular interests, along the lines of (or abusing) the 'just war' doctrine.[180]

It is thus difficult to accept that an armed reaction, whether called 'self-defence' or otherwise, is permitted against a State's lack of due diligence[181] in preventing cyber attacks from within its jurisdiction. This is not to imply, of course, that failure to prevent is not internationally unlawful, nor that peaceful remedies against it (such as countermeasures) are also prohibited. Even more difficult is to accept that an armed reaction against a State as a whole is permitted insofar as this is the only way to hit those private individuals who have launched an attack. Some links between the State—provided that there is a 'State'—and the individuals who have launched the attack have to exist. In other words, the whole debate should focus on the criteria of attribution actually adopted in international practice, which may well be different in different contexts, rather than on self-defence against 'pure' non-State actors.

10. SOME SCEPTICISM BY WAY OF CONCLUSION

It is almost a commonplace today in the literature to conceive of cyber attacks, under certain circumstances, as 'use of force', 'armed attack' and/or 'armed conflict'.[182] This approach is aimed at identifying an appropriate legal framework and, typically, at justifying or 'legitimizing' cyber and kinetic actions or reactions of various kinds while prohibiting others. Cyber space is imagined as a battle space similar to physical space in which hostilities can be conducted similarly to acts performed in physical space. An effect-based interpretative approach is often preferred to others in order to conclude that certain cyber operations are 'equivalent' to kinetic operations, for either 'use of force' or 'armed attack' or 'armed conflict' purposes, and are therefore subject to the same legal regime. Some hopefully healthy scepticism on this narrative is not out of place.

Analogies and speculative conjectures abundantly feed the debate to the point of sounding often artificial. Internet has little to do with 'space', however this is defined,[183] and shares no analogy with kinetic activities carried out in physical space, although its use may produce grave consequences in the physical world. No doubt crimes may be committed through cyber operations, even amounting to international crimes, but in an inter-State (rather than imperial) global world, crimes fall in principle within the State law-enforcement paradigm. This is, for example, the approach to cyber attacks adopted by Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems.[184] The obvious objections to this argument are that criminal prosecution by one or another State and existing treaties may prove inadequate while the consequences of a cyber attack may be highly destructive.[185] Moreover, faced with a devastating cyber attack the UN Security Council may not be willing or may not reach the consensus to take measures under Chapter VII of the

---

[180] Focarelli (n 128) 358–62.
[181] See Antonopoulos (Ch 6 of this Handbook).
[182] For a valuable exception, see O'Connell (n 4).
[183] See n 8.
[184] See Directive 2013/40/EU of the European Parliament and of the Council (n 101).
[185] Tikk and others (n 35) 29.

Charter.[186] Finally, in his 2018 speech on 'Cyber and international law in the 21st century' the UK Attorney General insisted that:

> if we stay silent, if we accept that the challenges posed by cyber technology are too great for the existing framework on international law to bear, that cyberspace will always be a grey area, a place of blurred boundaries, then we should expect cyberspace to continue to become a more dangerous place.[187]

The counter-objection is that analogical reasoning in use of force contexts are quite perilous. The appeal to existing international law on the use of force may disguise, given the high uncertainty of the analogised rules deemed to be applied, the willingness of a few strong States to free ride 'legitimately' with no really constraining rules. The very basic concepts relied on to trigger the applicability of the international law on the use of force ('use of force', 'armed attack' and 'armed conflict') do not coincide even where they are defined by one and the same word. For example, the term 'attack' refers to a particular category of military operations under Article 49(1) of the 1977 Additional Protocol I to the 1949 Geneva Conventions, whereby 'attacks' are 'acts of violence against the adversary, whether in offence or in defence', which has a different legal meaning from the same word used in Article 51 US Charter. The notions of 'use of force', 'armed attack' and 'armed conflict' and their different meanings in different legal settings, together with their inferred 'equivalents' in cyber space, make 'upstream' the whole picture quite aleatory despite the possible soundness of 'downstream' deductions made to identify the rules applicable to one or another hypothetical scenario. The analogy instrument is here questionable in itself; the parameters of the analogies made are uncertain even in their kinetic context; and the effect-based test concerning the notion of 'armed attack' may in fact lead to several very different conclusions depending on the circumstances. It seems that only a case-by-case assessment of the overall perception by the international community as a whole can reasonably be expected. Besides, the more likely scenario is an armed response in kinetic terms to a cyber attack attributed to private individuals or groups, although very difficult if not impossible to attribute to a State, and here again the rules analogised are themselves very open to doubt even in their original conventional scenario.

The way forward seems to be the negotiation and creation of ad hoc international institutions and rules for the Internet. It has been suggested that cyber attacks can properly be viewed as violations of the non-intervention principle; as such, they would not justify self-defence but, as international unlawful acts, alternative *non-forcible* responses or coercive measures, possibly defensive, such as countermeasures or measures adopted or authorized by the UN Security Council.[188] The regulation of the Internet is no doubt highly problematic and involves

---

[186] There seems to be little doubt that the Security Council may use its discretion and determine that a certain cyber attack amounts to a 'threat to the peace' or even to an 'act of aggression' or a 'breach of the peace' according to Art 39 UN Charter, and take 'enforcement measures' (peaceful sanctions or military response) against the 'source' of the cyber attack, whether a State or a non-State actor. The Council may presumably also take 'cyber sanctions' or impose a 'cyber blockade' and it may arguably authorize the use of kinetic force, although Art 42 reads 'by air, sea, or land forces' which literally would exclude cyber attacks. See Marco Benatar and Kristof Gombeer, 'Cyber sanctions: Exploring a blind spot in the current legal debate' in *4th European Society of International Law Research Forum* (Estonia, 27-28 May 2011) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989786 accessed 7 February 2020.

[187] See n 49.

[188] O'Connell (n 4) 199 and 202–6; Buchan (n 44) 221–7; Roscini (n 51) 110–11.

a huge variety of complex issues, including the corporate private sector as well as States and non-State actors concerned with online censorship. At the same time some regulation is clearly necessary, hopefully one in line with international human rights standards. Efforts should be redoubled to raise global awareness of the scale and effects of crimes committed in the Internet, especially against critical infrastructure, so as to take appropriate coordinated steps in preventing and punishing them just as has been done in respect of other very serious transnational crimes, including international crimes. No 'global policeman' can really and effectively patrol the Net.

Clearly, there is an underlying logic of escalation in cyberwar. The more a State resorts to cyberspace to get more competitive and stronger vis-à-vis other relevant actors, the more it becomes vulnerable to cyber attacks, the more it will feel in danger and be inclined to 'equate' cyber attacks to kinetic attacks so as to 'legitimately' respond militarily. Most importantly, even assuming that States will exceptionally apply the existing rules on self-defence described above, they have to meet the necessity requirement concerning their continuing obligation to implement passive and active (short of prohibited 'force') electronic defences prior to the alleged cyber attack and be as far as possible in a position to avoid kinetic force to defend themselves from cyber operations.[189]

What is then the 'cyber use of force' debate hugely developed in recent years for? In addition to trying hypothetically to identify reasonable rules, the key purpose so far is twofold: *deterring* possible attacks and *promoting* the rules which could possibly govern major cyber attacks at the moment when they occur so as to have at that very moment the international community 'prepared' to share the view that the attack is indeed 'equivalent' to a kinetic attack which justifies a kinetic response. By disseminating the opinion that the law is the one found in most official statements and publications, their authors and sponsors are contributing to the belief that this 'is' the law. This institutional and doctrinal campaign may prove successful and shape the law in the future, perhaps and hopefully for the better, although this is different and should be kept distinct from the law as it stands.[190]

[189] On reducing vulnerability see Jeffrey S Katz, 'Smart grid security and architectural thinking' (White Paper, *IBM*) http:// www.smartgrid.gov/files/Smart_Grid_Security_Architectural_Thinking_201012.pdf accessed 7 February 2020.

[190] For a socio-constructivist approach to international law along these lines, see Focarelli (n 128).

16. Cyber-peacekeeping and international law

Nicholas Tsagourias and Giacomo Biggio

1. INTRODUCTION

Over the years, peacekeeping has become one of the main tools used by the United Nations (UN) and other security organisations for conflict prevention and management and for post-conflict reconstruction. Peacekeeping attains these objectives by physically deploying military and civilian personnel in conflict zones who implement a multitude of tasks through peaceful means but, if necessary, also through forcible means. Peacekeeping has always adapted to the changing nature of conflict and to changing perceptions as to how peace can be maintained.

Cyberspace and cyber tools can support existing conflicts or even amplify them. At the same time, cyberspace and cyber tools can facilitate the maintenance of peace and security which, as was said, are the main tasks of peacekeeping operations. 'Cyberizing' peacekeeping thus offers many opportunities by facilitating the effective and efficient implementation of various peacekeeping tasks. It however calls for changes or adaptations in the institutional, political, and legal framework supporting peacekeeping as well as changes in strategic, operational and tactical thinking. It is for this reason that in our opinion cyber-peacekeeping (CPK) as a new and evolving field requires serious legal and political analysis.

This chapter responds to this call and perhaps is the first major legal exploration of the concept of cyber-peacekeeping. It identifies peacekeeping tasks that can be cyberized; considers how international law applies to CPK; identifies certain technical, institutional, political and legal challenges facing CPK; and makes proposals as to how these challenges can be addressed. Although the discussion will focus on UN peacekeeping, it is also relevant to peacekeeping operations deployed by other organizations.

The chapter is structured as follows. Section 2 provides a brief overview of the institution of peacekeeping, its legal basis under the UN Charter and explains its constitutional principles of consent, impartiality, and use of force in self-defence. Section 3 introduces the concept of 'cyber-peacekeeping'[1] by identifying the activities associated with peacekeeping which can be 'cyberized' that is, performed through cyber means. It explains at the same time the benefits of incorporating cyber technologies to peacekeeping operations and considers certain technical, political, and legal challenges that arise as well as how the principles of consent and impartiality can be impacted when peacekeeping tasks are 'cyberized'. Section 4 examines

[1] See A Walter Dorn, *Keeping Watch: Monitoring, Technology and Innovation in UN Peace Operations* (United Nations University Press, 2011); A Walter Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations: Providing for Peacekeeping No. 13* (2016); Michael Robinson *et al*., 'An Introduction to Cyber Peacekeeping' (2018) 114 *Journal of Network and Computer Applications* 70. For a legal perspective on the topic, see Jann Kleffner and Heather Harrison Dinniss, 'Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations' (2013) 89 *International Law Studies* 512.

the legal framework that applies to the use of lethal force by cyber-peacekeepers in situations characterized by the absence of armed conflict; whereas Section 5 examines the legal issues pertaining to the use of lethal force in situations of armed conflict. Section 6 discusses certain structural and institutional challenges and provides recommendations as to how they can be addressed, and finally, Section 7 offers the authors' concluding thoughts.

2. PEACEKEEPING: DEFINITION AND LEGAL BASIS

Peacekeeping denotes operations 'undertaken to preserve peace, however fragile, where fighting has been halted and to assist in implementing agreements achieved by the peacemakers'.[2] Peacekeeping has been an integral part of the UN's peace and security mechanism with the first peacekeeping mission deployed as early as 1948.[3] Since then, there have been more than 70 missions, with 13 missions being active at the time of writing, deploying more than 95,000 personnel.[4] A UN peacekeeping operation (PKO) consists of civilian and/or military personnel operating under UN command.

Peacekeeping is not mentioned in the UN Charter, but its legal basis can be found in the doctrine of implied powers as explained by the ICJ for the first time in its *Reparation for Injuries* Advisory Opinion.[5] In the *Certain Expenses* Advisory Opinion the Court specifically addressed the lawfulness of peacekeeping operations established by the UN General Assembly (GA) by holding that Article 11 of the UN Charter 'empowers the General Assembly, by means of recommendation to States or to the Security Council, or to both, to organize peacekeeping operations, at the request, or with the consent, of the States concerned'.[6] The Court also opined that peacekeeping is a means for attaining the UN purposes of maintaining international peace and security.[7]

It follows from this that the GA can establish a PKO on the basis of implied powers that derive from its express powers in matters relating to international peace and security.[8] In the same vein, the Security Council (SC) can create peacekeeping operations in order to fulfil its 'primary responsibility for the maintenance of international peace and security'.[9] More specifically, the SC can recommend the establishment of a PKO in the exercise of its Chapter VI

---

[2] United Nations, *United Nations Peacekeeping Operations: Capstone Doctrine* (January 2008) http://pbpu.unlb.org/pbps/library/capstone doctrineNg.pdf (Capstone Report). On peacekeeping see Rosalyn Higgins, Phillippa Webb, Dapo Akande, Sandesh Sivakumaran and James Sloan, *Oppenheim's International Law: United Nations* (OUP 2017) Chapter 27; Bruno Simma, Daniel-Erasmus Khan, Georg Nolte and Andreas Paulus (eds), *The Charter of the United Nations: A Commentary* (OUP 2012) 1171–99.

[3] UNTSO (UN Truce Supervision Organization in Palestine), UN Doc S/RES/50 (1948) S/801.

[4] See https://peacekeeping.un.org/en/what-is-peacekeeping (the figures are valid as of April 2020).

[5] *Reparation for Injuries Suffered in the Service of the United Nations*, Advisory Opinion [1949] ICJ Rep 12.

[6] *Certain Expenses of the United Nations (Article 17, Paragraph 2, of the Charter)*, Advisory Opinion [1962] ICJ Rep 151, 164.

[7] Charter of the United Nations, 26 June 1945, UNCIO 15,335, art 10 ('UN Charter'); *Certain Expenses* (n 6) 163–8.

[8] See arts 10, 11, 12 and 22 of the UN Charter.

[9] Ibid., art 24.

powers with regard to the peaceful settlement of disputes.[10] It can also establish PKOs as part of its Chapter VII powers to maintain or restore international peace and security.[11] In the latter case, Article 41 of the UN Charter can provide a more concrete basis for PKOs established by the SC. This article empowers the SC to take various measures not involving the use of force in order to maintain or restore international peace and security.[12] As will be explained later, peacekeeping does not amount to an Article 42 peace enforcement operation and, therefore, Article 41 can form its legal basis.

Peacekeeping is defined by three cardinal or else constitutional principles: consent of the host State; neutrality/impartiality; and the non-use of force except in self-defence.[13] These principles reflect the fact that peacekeeping emerged as a substitute to hard and top-down security introduced by the UN Charter which never materialised. Its aim instead is to achieve a political solution to disputes with the cooperation of the parties.[14]

This immediately reveals the importance of the first principle, namely, host State consent. Consent is important not only from a political but also from a legal perspective as far as the establishment and/or deployment of the force is concerned. To explain, if the GA recommends the establishment and deployment of a PKO, host State consent provides the legal basis for its establishment and deployment since the GA lacks mandatory and enforcement powers. Otherwise, it will violate Article 2(7) of the UN Charter which prohibits UN interference in the domestic affairs of States.[15] To give an example, UNEF, the UN operation in Egypt, was established by the GA and was deployed on Egyptian territory after Egypt granted its consent and following Israel's refusal to have it deployed on Israeli territory. It was withdrawn when Egypt revoked its consent in 1967.[16]

Likewise, host State consent provides the legal basis for the establishment and deployment of a PKO recommended by the SC. In relation to PKOs established by the SC on the basis of a Chapter VII binding resolution,[17] host State consent is not necessary for the establishment of the operation but is necessary for its deployment. This is because peacekeeping is not an Article 42 enforcement operation exempted from Article 2(7) of the UN Charter and without consent, its deployment will violate that Article as mentioned previously.

---

[10] Ibid., art 36.

[11] Ibid., arts 39–42.

[12] Ibid., art 41. See also *Prosecutor v. Dusko Tadić (*Decision on the Defence Motion on Interlocutory Appeal Jurisdiction), Case No. IT-94-I (2 October 1995) para 35; *Certain Expenses* (n 6) 166, 171.

[13] UN, General Assembly Security Council, *Report of the Panel on United Nations Peace Operations* (21 August 2000) UN Doc A/55/305-S/2000/809 (Brahimi Report), para 48, which characterises them as 'bedrock' principles of peacekeeping, available at: https://www.un.org/ruleoflaw/files/brahimi%20report%20peacekeeping.pdf; UN, *Uniting Our Strengths for Peace: Politics, Partnership and People: Report of the High-Level Independent Panel on United Nations Peace Operations*, 16 June 2015 (HIPPO Report) para 121, which characterises them as 'core' principles, available at https://peaceoperationsreview.org/wp-content/uploads/2015/08/HIPPO_Report_1_June_2015.pdf. See further Nicholas Tsagourias, 'Consent, Neutrality/Impartiality and Self-Defence in Peacekeeping: Their Constitutional Dimension' (2006) 11 *Journal of Conflict and Security Law* 465.

[14] Ibid., 469.

[15] UN Charter art 2(7); Leland M Goodrich, 'The United Nations and Domestic Jurisdiction' (1949) 3 *International Organization* 14.

[16] GA Res 997 (ES-I); GA Res. 998 (ES-I), GA Res 1000 (ES-I); GA Res 1001 (ES-I) and *Report of the Secretary-General on the Withdrawal of the United Nations Emergency Force*, U.N. Doc A/6730 (1967) paras 60–70.

[17] UN Charter, art 25 in conjunction with art 103; Tsagourias (n 13) 471, 477.

Peacekeeping operations must also conform to the principles of neutrality and/or impartiality. The principle of neutrality alludes to the apolitical character of the operation. It means that the PKO should not take sides and should not alter the course of the events. Impartiality instead is an operational term and refers to the conduct of the operation.[18] It means that a PKO should execute its tasks in an impartial manner in accordance with the mission's mandate.[19] Although neutrality was important in the early days of peacekeeping, the evolution and complexification of peacekeeping have undermined the principle of neutrality and highlighted the importance of the principle of impartiality which has now become central to peacekeeping.

Finally, force must be used in personal self-defence or in the defence of others (such as civilians). Again, the scope of this principle expanded to also cover the defence of the operation's mandate.[20] The principle that force should be used in self-defence is critical in distinguishing a PKO from a peace-enforcement operation. The latter is launched against the will of the targeted State, it is not neutral or impartial, and the use of force is central to the operation. In peacekeeping however, the use of force is incidental and limited to achieve the mandate's specific objectives. Even if the use of force in peacekeeping is nowadays authorised by the SC, this does not transform it into a peace--enforcement operation. The SC is authorizing such uses of force because it is the only institution that can lawfully authorize any use of force which is not within the bounds of personal self-defence. Otherwise, such uses of force would be unlawful. That having been said, the boundaries with peace enforcement are quite thin, particularly in the case of robust operations. [21]

Having provided a brief overview of the institution of peacekeeping we now turn to an examination of what peacekeeping activities can be cyberized.

3. CYBER-PEACEKEEPING ACTIVITIES

Over the years, the mandates of PKO have expanded from the supervision of ceasefires to administering territories, protecting civilians, implementing peace agreements, monitoring elections, providing humanitarian assistance, protecting human rights, disarmament, neutralizing combatants.[22] This means that peacekeeping mandates have become multi-dimensional and, for this reason, peacekeepers can use different means and methods to fulfil their mandate. Moreover, PKOs are nowadays deployed in complex and high-risk environments.

---

[18] Brahimi Report (n 13) paras 48–50; Capstone Report (n 2) para 33.

[19] Tsagourias (n 13); Jane Bolden, 'Mandates Matter: An Exploration of Impartiality in United Nations Operations' (2004) 11 *Global Governance* 147; Hikaru Yamashita, 'Impartial Use of Force in United Nations Peacekeeping' (2008) 15 *International Peacekeeping* 615; Emily Paddon Rhoads, *Taking Sides in Peacekeeping: Impartiality and the Future of the United Nations* (OUP 2016).

[20] See Brahimi Report (n 13) paras 48–51 and HIPPO Report (n 13) para 125. See also Scott Sheeran, 'Use of Force in United Nations Peacekeeping Operations' in Marc Weller (ed), *The Oxford Handbook of the Use of Force in International Law* (OUP 2011); Nicholas Tsagourias, 'Self-Defence, Protection of Humanitarian Values, and the Doctrine of Neutrality and Impartiality in Enforcement Mandates' in Weller, ibid; *Leuven Manual on the International Law Applicable to Peace Operations* (CUP 2017) 145–56.

[21] For example, in relation to the Force Intervention Brigade. See UNSC Res 2098 (28 March 2013), UN Doc. S/RES/2098, para 12(b).

[22] Capstone Report (n 2) 23–24; Field Missions Mandate Table (2019) https://www.un.org/securitycouncil/file/122688.

Incorporating and using cyber technologies would thus enhance the ability of PKOs to carry out their task and implement their mandates more efficiently and effectively. To explain, PKOs would require less human, material or financial resources; their performance would be affected less by adverse conditions such as remoteness, inaccessibility, armed conflicts or security threats; the performance of their tasks would not always be dependent on the government's or other actor's attitudes; the collection and exchange of information and the communication between peacekeeping personnel and HQ will be faster, timely, and effective; decisions could be faster and more informed; the geographical or personal reach of their operations could expand without stretching their human or material resources; their personnel could be protected better from attacks because of better information, situational awareness, early detection of dangers or just remoteness; and last but not least local civilians could be protected better for the same reasons.

The UN has recognized that its PKOs are lagging behind States in the technologies they use and has tried to address this situation. The Report of the Independent High-Level Panel on Peace Operations states that incorporating new technologies in peacekeeping is an area of reform and that the immediate focus should be to introduce 'essential "enabling" technologies, as well as new approaches to improve: (i) safety and security; (ii) early warning and protection of civilians-related capabilities; (iii) health and well-being; and (iv) shelter and camp management'.[23] The Report also endorses the recommendations of the Expert Panel Report on Technology and Innovation in United Nations Peacekeeping (2015).[24]

Following these reports, the UN introduced the Digital Blue Helmets programme which forms a platform for the exchange of information and the coordination of protective or defensive action against cyber threats to the UN.[25] It also established the Department of Operational Support in 2019 which includes the Office of Information and Communications Technology.[26] This Department is responsible for developing and implementing the UN's ICT strategy through 'modernization, transformation and innovation and by providing a framework for improved governance, strong leadership and optimal use of information and communications technology resources.'[27] One of its initiatives is the Partnership for Technology in Peacekeeping whose objective is to empower PKO through the use of technologies.[28]

That having been said, the 'cyberization' of PKOs is still in a nascent stage. In what follows we will provide an overview of peacekeeping tasks that can be 'cyberized', and also identify potential legal, technical, and political challenges.

---

[23] Report on the Independent High-Level Panel on Peace Operations, UN Doc A/70/95 S/2015/446 (17 June 2015) paras 285–287, https://peacekeeping.un.org/en/report-of-independent-high-level-panel-peace-operations.

[24] Final Report of the Expert Panel on Technology and Innovation in UN Peacekeeping (2015) https://peacekeeping.un.org/sites/default/files/performance-peacekeeping_expert-panel-on-technology-and-innovation_report_2015.pdf.

[25] UN Digital Blue Helmets, https://unite.un.org/digitalbluehelmets/cyberrisk.

[26] https://operationalsupport.un.org/en/technology.

[27] UN Secretary General, 'Information and communications technology in the United Nations: Report of the Secretary-General', UN Doc A/69/517 (10 October 2014) https://digitallibrary.un.org/record/781647?ln=en.

[28] https://operationalsupport.un.org/en/partnership-technology-peacekeeping.

(i) Observation, Monitoring and Reporting of IHRL and IHL Violations

Observation, monitoring, and reporting ('OMR') is a standard peacekeeping task.[29] Likewise, monitoring networks and reporting cyber-attacks is a critical function in any organization nowadays and involves tools and methods to gather information about the source and type of attack, its destination, or its methodology; information which is necessary in order to defend systems and respond to such attacks.

In our opinion, cyber technology can be used for various OMR tasks and particularly in relation to human rights law (IHRL) and international humanitarian law (IHL) violations. It will enhance the effectiveness of OMR because cyber technology can overcome physical obstructions, expand the scope of monitoring and the scope of collected information; speed up the process of collection, analysis, and assessment; make more informed decisions; and take faster action.

In relation to IHRL, cyber-OMR can be used to detect possible violations of the right to life[30] or the right to liberty and security of person[31] which can be caused by kinetic means or by cyber means, such as a cyber-attack that is directed against a water distribution system and is intended to cause injury and/or death to civilians.

Cyber-OMR can also be used to detect violations of the right to privacy,[32] for example, cyber-attacks that exfiltrate personal data from governmental or private servers, ransomware and other types of attacks encrypting the victim's data.

Cyber-OMR can be used to verify whether the right to freedom of expression is respected in cyberspace[33] and that civilians are not denied access to certain information. For instance, cyber-peacekeepers may be tasked with monitoring social media to determine whether bots are spreading disinformation during an electoral campaign in favour of a party to the election and to the detriment of another. Moreover, by securing safe access into national Internet Service Provider (ISP), cyber-OMR can observe if a government is shutting down portions of the internet or whether it restricts or blocks access to certain websites.[34]

Cyber-OMR can be used to detect violations of the right of property.[35] Cyber-attacks may compromise or damage physical components of cyber infrastructure such as hardware. Furthermore, digital property may be damaged when a cyber-operation deletes or exfiltrates valuable data of a commercial nature. Cyber-peacekeeping can thus ensure the safety of

---

[29] According to the OHCHR:
> [m]onitoring is a broad term describing the active collection, verification and immediate use of information to address human rights problems. Human rights monitoring includes gathering information about incidents, observing events (elections, trials, demonstrations, etc.), visiting sites such as places of detention and refugee camps, discussions with Government authorities to obtain information and to pursue remedies and another immediate follow-up. The term includes evaluative activities at the UN headquarters or operation's central office as well as first-hand fact-gathering and other work in the field. In addition, monitoring has a temporal quality in that it generally takes place over a protracted period of time

OHCHR Training Manual on Human Rights Monitoring (2001) 9.

[30] UDHR art 3; ICCPR art 6; ECHR art 2; ACHR art 4.

[31] UDHR arts 3 and 9; ICCPR art 9; ECHR art 5; ACHR art 7.

[32] UDHR art 12; ECHR art 8; ICCPR art 17; ACHR art 11.

[33] UDHR art 19; ECHR art 10; ICCPR art 19; AHCR art 13.

[34] As suggested by Robinson (n 1) 8.

[35] UDHR art 17; ACHR art 14.

State-owned networks against hostile cyber-operations or those owned by private companies and thus prevent or supress tensions among the actors involved in the peace process.

In relation to IHL, cyber-OMR can be used to detect violations committed through conventional or cyber means by States or armed groups, in particular attacks on civilians or civilian objects.[36] In this regard, cyber-peacekeeping can implement cyber-surveillance measures by monitoring networks, websites and intercepting their personal communications in order to retrieve valuable information about the target of the attacks and whether they are civilians. Cyber technology can also be used effectively to store and share relevant data and information.

The scope and effectiveness of OMR in relation to IHL violations depends on how the term 'attack' is defined. In IHL it is defined as 'an act of violence against the adversary, whether in offence or defence' with violence being synonymous to physical harm.[37] Likewise, in the cyber context, it has been defined as 'any cyber operation which is reasonably expected to cause death or injury to individuals, damage or destruction to objects, or a combination thereof'.[38] OMR can thus focus on detecting cyber-attacks which would likely threaten the life of civilians or cause damage. In our opinion, the aforementioned definition is too restrictive because cyber-attacks can often cause serious adverse consequences without necessarily resulting in physical violence. To give certain examples, a cyber-attack may disrupt the supply of electricity within a State,[39] manipulate its stock market in order to adversely affect its economy, disrupt the distribution networks of an energy company,[40] exfiltrate social security related data of millions of civilians,[41] or prevent thousands of individuals and companies from accessing their computers until a ransom is paid.[42] Clearly, these are all instances of cyber-operations that do not necessarily result in physical damage but which can have negative consequences for the civilian population and can endanger the peace process since one of the peacekeeping tasks, as was said, is State reconstruction and the restoration of civilian life. We therefore submit that the notion of attack should also include cyber operations which adversely impact

---

[36] International Committee of the Red Cross (ICRC), *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, 8 June 1977, 1125 UNTS 3, art 48 (AP I); *Rome Statute of the International Criminal Court (last amended 2010)*, 17 July 1998, art 8 (ICC Statute).

[37] Art 49 AP I.

[38] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) Rule 92 and Commentary, 415.

[39] 'An Unprecedented Cyber Attack Hit US Power Utilities', *Wired* (9 July 2019) https://www.wired.com/story/power-grid-cyberattack-facebook-phone-numbers-security-news/.

[40] John Leyden, 'Hack on Saudi Aramco hit 30,000 Workstations, Oil Firm Admits', *The Register* (29 August 2012) https://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis/; Council on Foreign Relations, 'Compromise of Saudi Aramco and Ras Gas', *Cyber Operation Tracker* https://www.cfr.org/interactive/cyber-operations/compromise-saudi-aramco-and-rasgas.

[41] Brendan Koerner, 'Inside the Cyberattack That Shocked the US Government', *Wired* (23 October 2016) https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

[42] Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired* (22 August 2018) https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Critical National Infrastructure (CNIs).[43] Although States have adopted different definitions,[44] at a minimum, CNI includes those services which are deemed of such importance that their incapacitation or destruction 'would have a debilitating impact on security, national economic security, national public health or safety, environment'[45] and this fits with the broader State reconstruction aims of modern peacekeeping. Accordingly, cyber-OMR should include detection of cyber-attacks that may destroy CNI or disrupt their functionality.

Although cyber-OMR can be useful, the challenges it poses should not be underestimated. One such challenge relates to the volume of networks and their interconnections that should be monitored in order for cyber-OMR to be effective. Another challenge relates to the resources and forensic knowledge required for cyber-OMR. Conformity with human rights is another challenge because OMR can be quite intrusive and could degenerate into constant surveillance. Furthermore, cyber-OMR and in particular the monitoring of IHRL and IHL violations can adversely affect the consent of the government or local actors because it may reveal their IHRL and IHL violations. It may put the UN in the invidious position of either exposing these violations and perhaps be exposed to attacks; face uncooperative parties and demands to withdraw; expand the peacekeeping operation to deal with such violations; or remain silent and be accused of complicity in such violations. In addition to the above, cyber-OMR may raise questions about the type and amount of evidence required to establish violations, how such evidence is to be collated and assessed; what standard of proof should apply; and how cyber evidence can be corroborated with other evidence. Another challenge is the degree of human involvement in assessing information because, if Artificial Intelligence is used for example, it is not always possible to assess whether the taking of life was arbitrary or that death or injury to civilians was proportional in the complex situations where peacekeepers are deployed. For all these reasons, unless a clear framework for cyber-OMR is established with clearly defined competences, actions, and legal standards, cyber-OMR can be perceived by the parties as biased, it may strain the other peacekeeping principle, the principle of impartiality and, ultimately, it may hinder the effective implementation of the peacekeeping tasks.

(ii) Monitoring the Implementation of Cyber Cease-fire Agreements

Cyber-peacekeepers can also be employed to monitor the implementation of a cyber cease-fire agreement according to which parties have agreed not to launch cyber-attacks against each

---

[43] For a similar approach, see for instance Noam Lubell, 'Lawful Target in Cyber Operations: Does the Principle of Distinction Apply?' (2013) 89 *International Law Studies* 252, 263–73 (where the author argues that 'there is a need to reconsider the threshold of harm in light of the potential of serious non-physical harm'); Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014) 181.

[44] The Vice Chairman of the US Joint Chiefs of Staff, *Memorandum for Chiefs of the Military Services Commanders, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates* (2011) 5; Federal Ministry of the Interior, *Cyber Security Strategy for Germany* (February 2011) 15; UK Government, *National Cybersecurity Strategy 2016 to 2021* (11 November 2016) 73; Council of the European Union, *Council Directive 2008/114/EC on the identification and designation of European National Infrastructures and the assessment of the need to improve their protection'*, 8 December 2008, art 2 (a).

[45] Memorandum for Chiefs of the Military Services Commanders (n 44).

other.[46] This would require, first of all, the establishment of a 'cyber-safe layer' consisting of designated networks and systems[47] to be protected against cyber-attacks through the use of passive cyber-defence measures. The aim of these measures would be to improve network resilience and can include firewalls, encryption of files, patches of known vulnerabilities.[48] Secondly, cyber-peacekeepers can perform OMR activities on the 'cyber-safe layer' to verify that all cyber-attacks have ceased. If necessary, cyber-peacekeepers can also implement active cyber-defence operations aimed at repelling or deterring future cyber-attacks, as well as destroying and removing malware. Finally, cyber-peacekeepers can share information with relevant parties relating to what systems have been compromised and whether valuable information has been stolen.

The successful monitoring of a cease-fire agreement primarily depends on the clarity of the terms of the agreement. In our opinion, the parties to a cyber cease-fire agreement should define what amounts to a 'cyber-attack' on the basis of the anticipated consequences that a hostile cyber-operation might have on networks, systems and cyber infrastructures that are critical for the maintenance of peace and such definition would not necessarily require only physical damage. For instance, loss of functionality can be included as explained previously.

The consent of the government and all other parties is also important for the effective monitoring of a cease-fire agreement. However, the government may be reluctant to share information related to its own networks, if doing so would reveal potential vulnerabilities to other parties involved in the agreement or to the troop contributing countries.

The resources and forensic knowledge required is another challenge for monitoring cyber cease-fire agreements but also for the capacity to restore affected services.

The effectiveness of a cyber cease-fire agreement also depends on identifying the perpetrators of a cyber-attack. However, attribution of cyber-attacks is notoriously problematic.[49] From a technical perspective the interconnected nature of cyberspace allows the perpetrators to route a cyber-attack through multiple servers which can be located anywhere within the territory of a State, or across several States which may however be unwilling to cooperate with cyber-peacekeepers.[50] While techniques such as digital forensics and malware analysis can succeed in linking the cyber-attack to its perpetrator, the political costs associated with erroneous or inaccurate attribution cannot be underestimated as it can undermine the legitimacy of cyber-peacekeepers and alienate the parties. Additionally, the legal challenges and costs

---

[46] In relation to conventional peacekeeping see United Nations Iran–Iraq Military Observer Group (UNIIMOG); United Nations Good Offices Mission in Afghanistan and Pakistan (UNGOMAP); United Nations Mission of Observers in Tajikistan (UNMOT); Liberia (UNOMIL); Angola (UNAVEM III and MONUA); Sierra Leone (UNOMSIL and UNAMSIL); and Guinea-Bissau (UNOGBIS).

[47] Michael Robinson *et al.*, 'Developing Cyber Peacekeeping: Observation, Monitoring and Reporting' (2018) *Government and Information Quarterly* 1, 10–2.

[48] James P Farrell and Rafal Rozinski, 'The New Reality of Cyber War' (2012) 15 *Survival* 107, 109 (defining passive cyber defence as measures of:

> cyber 'hygiene' that trains an educated workforce to guard against errors or transgressions that can lead to cyber intrusion, detection technology, 'honey pots' or decoys that serve as diversions, and managing cyberspace risk through collective defence, smart partnerships, information training, greater situation awareness, and establishing secure, resilient network environments.

[49] See Nicholas Tsagourias, 'Cyber Attacks, Self-defense and the Problem of Attribution' (2012) 17 *Journal of Conflict and Security Law* 229; Nicholas Tsagourias and Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges' (2020) 31 *European Journal of International Law* 941.

[50] Robinson (n 1) 17.

cannot be discounted because attribution would require trans-jurisdictional activities for which the UN should obtain the consent of those States whose jurisdictions are involved in such enquiries. In view of these challenges, attribution poses a barrier that might prove difficult to overcome.

(iii) Introducing and Monitoring Cyber Buffer Zones

Installing and monitoring a buffer zone is a core peacekeeping activity, with the one established in Cyprus being the most long-standing.[51] A buffer zone is a demilitarized zone monitored by peacekeepers where attacks are prohibited. The overall aim is to prevent the recurrence of violence by keeping the conflicting parties apart.[52] The same rationale can apply to cyber-peacekeeping where cyber-buffer zones covering specific networks (for instance those supporting Critical National Infrastructure) will be protected from cyber-attacks through the use of offensive cyber-defence techniques.[53] These measures can, for instance, include the 'disabling of servers, networks, and computers that are responsible for hosting and distributing the attacking code'.[54]

There are considerable benefits in creating cyber-buffer zones because civilians and civilian infrastructure will be protected from attacks and the State will be able to function since its essential infrastructure will remain operational. It will assist in the restoration of civilian life which is one of the tasks of a PKO. However, cyber-buffer zones also give rise to questions as to whether CNI networks can be separated from general networks, and whether governments would consent to have their infrastructure being monitored by cyber-peacekeepers.

(iv) Cyber-disarmament

Another important function of cyber-peacekeeping is the performance of cyber-disarmament duties. While this task is undeniably valuable, its effective implementation faces several difficulties. The first and foremost is definitional. There is presently no settled legal definition of 'cyber-weapon' and this affects the scope and utility of any disarmament task. It seems quite intuitive to compare cyber-weapons to conventional weapons, which are described as 'means to commit acts of violence against human or enemy forces'.[55] However, such a definition is too restrictive and would be ineffective in the context of cyber disarmament. In fact, there are few cyber-weapons that can cause physical violence. So far, the most disruptive cyber-weapon has been Stuxnet and no other cyber-weapon has risen to that level of physical violence.[56]

---

[51] See UNSC Res 186 (1964) establishing UNFICYP, https://unficyp.unmissions.org/.

[52] In IHL there is the notion of protected zones or demilitarized zones; see Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law* (CUP 2005) Rules 35 and 36; Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces, art 23; Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War, arts 14(1) and 15; AP I, art 60(3).

[53] Nicholas Tsagourias and Russell Buchan, 'Automatic Cyber Defence and International Law' (2017) 60 *German Yearbook of International Law* 1.

[54] Ibid., 3.

[55] Henckaerts and Doswald-Beck (n 52) Rules 6, 23.

[56] Nicholas Falliere *et al*., 'W32.Stuxnet Dossier', *Symantec Security Response* (November 2010) https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf. With the exception

Instead, more common are cyber-weapons aimed at causing effects which are not violent but are, nonetheless, severely disruptive. It is thus submitted that the definition of 'cyber-weapon' should be extended to include malware which can cause severely disruptive consequences, even if they do not rise to the level of injury or death.

The second difficulty has to do with the fact that, whilst conventional weapons are entirely physical objects, cyber weapons are primarily virtual objects made of malicious code which then can be stored in different devices. This qualitative difference has a defining impact on disarmament methods and procedures.

Traditionally, one key aspect of the disarmament process has been the verification and the identification of the location of weapons through On-Site Inspections (OSIs). Considering that the success of OSIs depends on the fact that there are only so many designated sites, it cannot be effective in the case of cyber-weapons because, as we said, they are not physical, and they cannot be easily located. Cyber-weapons can be stored anywhere within a State's networks, they can be saved in an external hard drive or USB stick, or be encrypted to avoid detection. They can also be developed by individuals that might not even be within the territory of the State that is being inspected. In light of this, a viable solution would be the employment of cyber investigation measures in relation to selected computers and networks. A cyber investigation involves the use of 'network taps' in order to perform activities of sessions reconstruction, log inspection and traffic analysis which includes the cross-analysis of packets of data to determine what kind of information has been shared between two computers and whether or not abnormal activity within the surveyed networks has been detected. By doing so, cyber-peacekeepers should be able to effectively verify and monitor whether a party is developing malicious software.

Once the malware has been identified, disarmament efforts must necessarily be adapted to the cyber context. Unlike the conventional context, where a weapon has to be taken away from its owner and then disassembled, if a malware is dismantled it can still proliferate with ease, for instance, by being downloaded voluntarily or involuntarily by users or by simply being made available to the wider public, as it happened with the source code of Stuxnet. A possible solution, at least from a technical point, would be for the cyber-peacekeepers to obtain the source code of the malwares in order to develop effective countermeasures to neutralize it. This will prevent future deployment of the malware by the parties or external actors. This approach, however, may face political barriers that might prove difficult to overcome. States or other parties may not give their consent. A more realistic option may consist of shifting the focus from the cyber-weapon to the target. By concentrating on passive cyber-defence, the cyber-peacekeeping contingent can work closely with local parties in order to improve the resilience of their networks, for instance by patching known vulnerabilities and by implementing firewalls.

---

of an incident that lead to the explosion of an oil pipeline in Iran, which was allegedly attributed to a cyber-attack launched by a yet unknown agent. See in this regard Kayrmin Serjoie, 'Iran Investigates if Series of Oil Industry Accidents Were Caused by Cyber Attack', *Time* (12 August 2016) https://time.com/4450433/iran-investigates-if-series-of-oil-industry-accidents-were-caused-by-cyber-attack/.

(v) Electoral Assistance

Electoral assistance is one of the tasks of modern peacekeeping. It includes ad hoc assistance to hold credible elections as well as building State capacity to hold elections. The overall aim is to foster democratic rule. Cyber-peacekeepers can thus engage in building cyber election infrastructure which can be easier and less costly than developing physical election infrastructure. However, a lot depends on the available resources at the local level. Cyber-peacekeepers can also protect the electoral process from attacks, for example attacks on the electronic voting system. That said, it must be pointed out that such a scenario may be quite ambitious since States that tried to introduce electronic voting abandoned it due to security concerns.[57]

Where cyber-peacekeeping can be more effective is in providing assistance to combat the spread of disinformation and misinformation during the electoral process. This can be done by protecting networks from hacking and detecting spam bots on social media that disseminate disinformation. Combating disinformation and misinformation is important for creating a democratic space and for preventing conflict since the aims of disinformation and misinformation is to foment conflict and division.

(vi) Governance Functions

Often peacekeepers have been entrusted with governance functions, not only by providing security and policing, but also by establishing governing institutions or by effectively running a State. For example, peacekeepers may be involved in developing utilities and basic services such as tax revenue and hospitals. Beyond that, they can also perform administrative, legislative and judicial functions as it happened in Kosovo or East Timor. This means that many aspects of State functions can be cyberized such as those related to taxation, legal and judicial transactions, administration tasks, education, health care, social security and welfare, policing, banking. Of course, this would require the necessary technological resources at the peacekeeping and local level; human capacity but also the existence of comprehensive and effective political and legal system at the local level.

4. THE USE OF LETHAL FORCE IN CYBER-PEACEKEEPING OUTSIDE AN ARMED CONFLICT SITUATION

In this section we will consider the legal framework that applies to the use of lethal force by cyber-peacekeepers outside an armed conflict situation and the challenges that arise. As was already said, peacekeepers can use limited force in personal self-defence and in the defence of civilians. In the absence of an armed conflict, the use of lethal force is regulated by the laws of the sending State, the laws of the host State, the relevant SC resolutions, the ROE, and IHRL which usually informs the former. According to IHRL, the use of lethal force should

[57] Josh Lowe, 'Netherlands Abandons Electronic Voting Counting Amid Hacking Fears', *The Register* (3 June 2017) <https://www.newsweek.com/dutch-election-electronic-voting-hacking-russia-france-macron-trump-clinton-564198>.

be absolutely necessary, proportionate, and comply with the duty to take precautions.[58] These requirements have acquired customary law status and thus apply to PKO and for that matter to cyber-peacekeeping.

Necessity describes a situation where the life of a peacekeeper is under imminent danger and the use of lethal force is the only option available to protect his/her life. This means that other, non-lethal alternatives (such as arresting the suspect), have been exhausted or are ineffective. The proportionality principle requires that force must be proportionate to the aim of protecting the life of the peacekeeper. Finally, the duty to take precautions acts as a logical corollary to necessity and proportionality by requiring from peacekeepers to plan their operations in such a way as to minimize the risk to others.

The same considerations apply to the use of lethal force by peacekeepers in order to protect civilians facing imminent danger. For example, the SC often authorizes the use of force to protect civilians 'under imminent threat of physical violence' and adds that they [peacekeepers] should use force 'within their capabilities'.[59] This formulation reinforces the view that the use of force should not exceed the requirements of necessity and proportionality and that it should be a last resort.

Although the same requirements would apply to cyber-peacekeeping, we should add two caveats. First, they will not apply to cyber-operations that are not intended to cause death or injury and thus exclude the majority of cyber-operations which as was said are not lethal. That having been said, it is also true that deciphering the lethal or otherwise intended harm of a cyber-operation is quite difficult, something that raises questions about the proper application of this criterion. Secondly, the circumstances under which cyber-peacekeepers may resort to lethal force to defend themselves are limited because cyber-peacekeepers can operate remotely or in ways that do not require their physical presence. For example, monitoring a cyber cease-fire agreement, providing electoral assistance, or reporting on human rights and IHL abuses are tasks that do not require physical presence and can be performed remotely.

That said, the following scenario will illustrate how the IHRL paradigm on the use of lethal force can apply to cyber-peacekeeping. It runs as follows. A cyber-peacekeeping operation is tasked with monitoring and protecting a cyber-buffer zone involving the cyber infrastructure of the State's water treatment facility which is part of its CNI. It becomes aware that a hacker is planning to launch a cyber-attack against the facility's software programme. If successful, the water will be poisoned, endangering the lives of a large portion of the population. In order to determine whether the use of lethal force would be lawful in this instance, the threat to civilians' life must be imminent. In order to establish imminence, there should be sufficient evidence indicating the existence of concrete intention and capacity to mount the cyber-attack. Once imminence is established, the cyber-peacekeeping force should exhaust all other non-lethal means to prevent the cyber-attack. For example, it can use active cyber defence measures aimed at stopping the cyber-attack by incapacitating the attacker's servers. Resort to cyber-operations causing physical, non-lethal, damage must also be considered, such as operations that destroy the system's hardware and thus make it inoperable. As a matter of fact, non-lethal cyber means can be quite effective. However, if non-lethal means are unfeasible or ineffective, resort to lethal force can be justified. Such force can be kinetic

---

[58] Siobhan Wills, 'Use of Deadly Force by Peacekeepers Operating Outside of Armed Conflict Situations: What Laws Apply?' (2018) 40 *Human Rights Quarterly* 663.

[59] See e.g., SC Res 1265 (1999); SC Res 1296 (2000); SC Res 1267 (2006); SC Res 1894 (2009).

or cyber; for example, by sending malware that make the computer or the mobile devices used by the hacker to explode, causing his/her death. Such use of lethal force will satisfy the requirement of necessity but also of proportionality because it will not exceed the objective of protecting people's lives. In addition to this, the obligation to take precautions would require cyber-peacekeepers to minimize the effects of lethal force in the planning phase of the cyber operation. More specifically, they should do everything necessary to avoid disrupting the functionality of networks, if doing so would result in physical harm to civilians, and they should contain the spread of the malware, for example via a self-destruction switch.

The next issue to consider is the application of the IHRL paradigm to cases where cyber-peacekeepers rely on active automatic cyber-defence. This involves AI-operated software with minimal human intervention in the operational phase[60] which actively pursues the hacker in his/her own systems. In the scenario at hand, the CPK's computer programmed to monitor the buffer-zone will react immediately after detecting a forthcoming cyber-attack by sending malware which kills the hacker. Would the requirements of necessity and proportionality be satisfied? In relation to necessity, the attack should be imminent and it is feasible for a computer to be programmed to recognize patterns of events that indicate that a cyber-attack is in progress.[61] In relation to the scenario discussed here, the computer can detect, for example, that the servers of the water supply network are being flooded with abnormally high amounts of access requests, a circumstance which can signal that an attack is underway. It must then determine whether active cyber-defence measures can comply with the principle of necessity. This is difficult because it needs to make determinations as to whether other measures, such as arrests, can be more effective. Also, in relation to proportionality, it should assess the effects caused on the attacker's network, computer, or cyber infrastructure in general and the effects on the surrounding human and physical environment. This requires knowledge and assessment of many variables which a computer cannot perform with the requisite degree of certainty without human input. For this reason, we can say that, although automatic active cyber defence can assist cyber-peacekeepers in many respects, it can also lead to wrong assessments if humans are out of the loop. This will furthermore have negative legal consequences but also affect host State's consent and tarnish the peace process.

5. THE USE OF LETHAL FORCE BY CYBER-PEACEKEEPERS DURING AN ARMED CONFLICT WHERE INTERNATIONAL HUMANITARIAN LAW APPLIES

In contrast to the IHRL paradigm of the use of lethal force discussed in the previous section, the IHL paradigm as *lex specialis*[62] centres around the principle of distinction which has customary law status.[63] According to this principle, combatants can be lawfully attacked at all

---

[60] Tsagourias and Buchan (n 53) 3.

[61] Ibid., 6–7.

[62] *Legality of the Threat or Use of Nuclear* Weapons, (Advisory Opinion) [1996] ICJ Rep 226, para 25; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) [2004] ICJ Rep 136, para. 106; *Case Concerning Armed Activities on the Territory of the Congo (*Merits) [2005] ICJ Rep 168, para. 216.

[63] Art 48 AP I. The principle of proportionality also provides certain limitations to the use of lethal force, but the principle of distinction is the one that offers primary protection.

times whereas civilians are protected from attacks, unless and for such time as they participate directly in hostilities (DPH).[64]

The questions to be examined in this section are: first, under what circumstances IHL applies to CPK; and second, what is the status of cyber-peacekeepers and under what circumstances cyber-peacekeepers can be lawfully attacked in view of the fact that a cyber-peacekeeping force may consist of military as well as civilian personnel.

With regard to the first question, IHL applies when there is an armed conflict. An armed conflict is defined by the resort to armed violence that is, the use of means and methods of warfare to cause death, injury, damage, or destruction.[65] The immediate question is whether loss of functionality, for example disabling a server or blocking a computer, can also give rise to an armed conflict. This will be the case if physical replacement is needed or if knock-on physical effects are produced.[66] However, as explained previously, an armed conflict should also arise if the loss of functionality is severe and involves CNI.

What is important for the application of IHL is not only the existence of an armed conflict but also its classification because it determines what specific law will apply. IHL recognises two types of armed conflict: an international armed conflict (IAC) which is a conflict between States or between States and armed groups under State control[67] to which the law of IAC applies; and, a non-international armed conflict (NIAC) which is an armed conflict of certain intensity[68] between a government and organised armed groups or between such armed groups to which the law of NIAC applies.[69]

It follows from the above that IHL will apply from the moment a PKO/CPK is involved as party to an armed conflict. It will become a party to an armed conflict if it resorts to armed force against another party (State or armed group) by launching, for instance, operations to destroy servers or networks; operations that cause death or injury; or operations that cause severe loss of functionality of critical infrastructure. To the extent that such operations produce these effects, are systematic, and war-like, they fall outside the scope of personal defence or the defence of civilians. Furthermore, depending on the character of the other parties, it will be the law of IAC or the law of NIAC that will apply to the exchanges between the cyber-peacekeepers and these parties.[70]

---

[64] Art 51(3) AP I and Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of Non-International Armed Conflicts (AP II), art 13(3). See further Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities* (ICRC, Geneva 2009) (DPH Guidance).

[65] ICTY, *Prosecutor v. Tadić*, (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction), Case No. IT-94-1-A, Appeals Chamber (2 October 1995) para 70; US, Department of Defense, *Law of War Manual*, Office of General Counsel (June 2015, updated 2016) para 3.3.1.

[66] Tallinn Manual 2.0 (n 38) Rules 82 and 83.

[67] Common Article 2 Geneva Conventions. See also 2016 Commentary, Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949, Article 2, paras 465–82, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=72239588AFA66200C1257F7D00367DBD; *Prosecutor v. Tadić* (n 65).

[68] ICTY, *Prosecutor v. Boškoski and Tarčulovski*, (Judgement), Case No. IT-04-82-T, Trial Chamber II (10 July 2008), paras 177, 197.

[69] Common Article 3 to the Geneva Conventions; AP 1, Art 1(1); *Prosecutor v. Tadić* (n 65).

[70] Nicholas Tsagourias and Alasdair Morrison, *International Humanitarian*: *Cases, Materials and Commentary* (CUP 2018) 36, para 9; *Leuven Manual* (n 20) 91–104; Tristan Ferraro, 'The Applicability

An interesting question is whether active cyber defence measures and, more specifically, automatic cyber defence measures can trigger an armed conflict. In our opinion, they can trigger an armed conflict if the conditions for its existence as described above are satisfied. That having been said, automatic cyber defence, in particular when humans remain 'out' of the loop, poses many challenges regarding the classification of the conflict because it is not easy to perform attribution and it is not easy to distinguish State-controlled systems from those controlled by armed groups.

The second question to consider is what is the status of cyber-peacekeepers in an armed conflict and under what circumstances they can be lawfully targeted. As was said, according to the principle of distinction, combatants can be lawfully targeted whereas civilians should be protected unless they directly participate in hostilities. The 1999 Bulletin by the UN Secretary-General makes the following statement:

> The fundamental principles and rules of international humanitarian law … are applicable to United Nations forces when in situations of armed conflict they are actively engaged therein as combatants, to the extent and for the duration of their engagement. They are accordingly applicable in enforcement actions, or in peacekeeping operations when the use of force is permitted in self-defence.[71]

This alludes to a concept of limited combatancy according to which peacekeepers can be targeted only as long as they act as combatants; the default position is that they are civilians.[72] In our opinion, this is unwarranted and can undermine the IHL principle of equality of belligerents. It also creates legal uncertainty as to whether the use of lethal force in the particular instance is regulated by the IHRL or the IHL paradigm. Furthermore, it strains the facts on the ground often characterized by intense exchanges of fire between peacekeepers and other parties.

For these reasons we submit that, if a CPK becomes a party to an IAC, its military contingent becomes combatants and can be lawfully targeted, whereas its civilian contingent remains protected from attacks unless they directly participate in hostilities (DPH). We also submit that they retain the status of combatant from the time they become a party to the armed conflict until the end of the armed conflict.[73]

In an NIAC where the principle of distinction does not apply formally, the ICRC defines civilians as those who are not members of a State's armed forces or those members of armed groups that have no continuous combatant function.[74] Whether membership to an armed group should be defined by function or by the act of membership is debated.[75] In our opinion, mem-

---

and Application of International Humanitarian Law to Multinational Forces' (2013) 95 *International Review of the Red Cross* 561. The fact that the PKO is deployed with the consent of the government does not change this finding because consent is relevant for the *jus ad bellum*.

[71] UN Secretary-General's Bulletin, *Observance by United Nations Forces of International Humanitarian Law* (6 August 1999) UN Doc ST/SGB/1999/13, 1.1. See also art 2(2), Convention on the Safety of United Nations and Associated Personnel, 2051 UNTS 363.

[72] See also SCSL, *Prosecutor v. Issa Hassan Sesay, Morris Kallon and Augustine Gbao ("the RUF Trial")*, Judgment, Case No. SCSL-04-15-T Trial Chamber I (2 March 2009) para 233; ICC, *Prosecutor v. Bahar Idriss Abu Garda,* (Decision on the Confirmation of Charges), Case No. ICC-02/05-02/09, Pre-Trial Chamber I (8 February 2010) para 83.

[73] Tsagourias and Morrison (n 70) 108, para. 8.

[74] DPH Guidance (n 64) 27–37.

[75] *Law of War Manual* (n 65) para 5.7.3.

bership and not function should be the correct criterion provided however that the group is organised.[76] In light of this, we submit that the military contingent of a PKO/CPK in an NIAC can be lawfully targeted from the moment the PKO/CPK becomes a party to that NIAC and until its end.

It should be noted at this junction that treating the military contingent of a PKO/CPK as combatants does not undermine the principle of impartiality. As we said, impartiality is an operational principle but whether an armed conflict exists and whether a party is a combatant is a factual issue that depends on whether there is resort to armed force. It does not depend on how force is used or the reasons for using force.

As far as the civilian personnel of a PKO/CPK is concerned, they will lose their protection if they commit DPH. It is therefore important to explain under what circumstances they may commit DPH in cyber-peacekeeping because, although the distinction between the military and civilian component in a traditional PKOs can be easily maintained, in CPK civilians can work alongside the military personnel as a team to support the military operations.

According to the ICRC's Interpretive Guidance to the Notion of Direct Participation in Hostilities[77] there are three cumulative requirements that must be met: first, the individual must engage in acts reaching a certain threshold of harm either by adversely affecting the military capacity of a party to the conflict or by causing injury or death to civilians or damage or destruction to objects;[78] second, such harm must be carried out in one single causal step (the so-called *direct causation* requirement);[79] and, third, there must be a *belligerent nexus* between the act and the armed conflict in that the act must be carried out with the intention to adversely affect one of the parties to the conflict.[80]

How do these conditions apply to CPK? For example, if civilian CPK personnel launch an attack which temporarily disables a network used by a party to the armed conflict or disrupts its electronic communications, these acts will satisfy the threshold of harm because they affect the cyber-capabilities of the targeted party. By contrast, if the attack disables or disrupts the civilian servers of a State which is not party to the armed conflict in order to affect an armed group which is party to an armed conflict, it will not satisfy this criterion unless the armed group's networks are connected to the State servers. Similarly, intelligence gathering will not satisfy this condition unless the intelligence gathering is linked to a specific harmful attack.

Regarding the second requirement namely, direct causation, the harm should be brought about in one causal step. Because such proximity is causal rather than temporal or geographic, remotely conducted cyber operations can satisfy this criterion.[81] However, many cyber operations will not satisfy this criterion. For example, cyber operations that produce delayed or

---

[76] Tsagourias and Morrison (n 70) 107 and 287–88, paras 4 and 5 respectively.

[77] DPH Guidance (n 64) 46–64. It should be noted that the ICRC criteria and their interpretation have not received widespread acceptance but in this chapter we use them as the basis of analysis. For the notion of DPH as applied to cyber armed conflict see David Turns, 'Cyber Warfare and the Notion of Direct Participation in Hostilities' (2012) 17 *Journal of Conflict and Security Law* 279; Heather Harrison Dinniss, 'Participants in Conflict: Cyber Warriors, Patriotic Hackers and the Laws of War' in Dan Saxon (ed), *International Humanitarian Law and the Changing Technology of War* (Brill 2013) 251–78; Roscini (n 43) 202–11; Tallinn Manual 2.0 (n 38) Rule 97 and Commentary.

[78] DPH Guidance (n 64) 47–50.

[79] Ibid., 51–8.

[80] Ibid., 58–64.

[81] Ibid., 55.

reverberating effects will be excluded and, as was said previously, this is what most cyber operations do. In view of the nature of cyber operations, we submit that the causal test must be interpreted more expansively to include all events in an uninterrupted causal chain of events and include any event which would not have happened 'but for' the event that immediately preceded it.[82] This means that second-order or third-order harm will suffice if it is linked to the cyber operation without the intervention of any other factor.

It also seems that logistics or software maintenance will not meet this test unless they are integral to the harmful act as will be seen later. The ICRC Interpretive Guidance has taken a more inclusive approach to composite acts which will satisfy this test if they are 'an integral part of a concrete and coordinated tactical operation that directly causes such harm'.[83] This would mean, for instance, that the civilian who develops a particular programme, provides training, and inserts the malware to the targeted system will be committing DPH together with the civilian cyber-peacekeeper who activates the malware and causes the damage if all these individual acts were integral and connected to the specific harmful act. Likewise, a civilian cyber-peacekeeper who does cyber reconnaissance to identify vulnerabilities in a network will be committing DPH if this operation is integral to a cyber-attack which disrupts that network. Had the above acts been assessed individually, it would have been difficult to link them to the harmful act.[84]

Regarding the third criterion of belligerent nexus, the harmful act must 'be specifically designed to do so [cause harm] in support of a party to an armed conflict and to the detriment of another'.[85] According to the ICRC Interpretive Guidance, personal self-defence and the defence of others are excluded.[86] Consequently, this test will not be met by civilian peacekeepers when they use force in personal defence or in the defence of civilians. It can also be said that, because of the principle of impartiality, any acts that fall within the peacekeeping mandate, including the use of force, are not in support of a party to the conflict. If this view is accepted, only acts that fall outside the peacekeeping mandate or acts that according to the mandate are for the benefit of one party and the detriment of the other will meet this test and constitute DPH.[87] However, as was said previously in relation to military contingents, the harm caused for the benefit or detriment of a party to an armed conflict is a factual issue and as the ICRC Interpretive Guidance states, what matters is the objective purpose of the act.[88] Consequently, any act by civilian peacekeepers that objectively harms a party to the armed conflict satisfies the test of belligerent nexus regardless of its subjective purpose or the intent of the peacekeeper.

---

[82] See Kenneth Watkin, 'Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" interpretive guidance' (2010) 42 *New York University of International Law and Politics* 641.

[83] DPH Guidance (n 64) 54–5.

[84] The US takes a broader view to also include acts that 'effectively and substantially contribute to an adversary's ability to conduct or sustain combat operations'; see *Law of War Manual* (n 65) para 5.8.3.

[85] Ibid., 58.

[86] Ibid., 61.

[87] The Force Intervention Brigade can be used as a tentative example. It was authorized to use force in cooperation with the national army to neutralize armed groups. UNSC Res 2098 (28 March 2013), UN Doc S/RES/2098, para 12(b); UNSC Res 2147 (28 March 2014), UN Doc S/RES/2147 para 4(b); UNSC Res 2211 (26 March 2015), UN Doc S/RES/2211, para 9(e). As was said however, the Force Intervention Brigade was actually an enforcement operation and it was military.

[88] DPH Guidance (n 64) 59.

Another issue that can cause difficulties is the temporal duration of DPH. According to the ICRC Interpretive Guidance, it includes preparatory measures, deployment, the act itself, and the actor's return and disengagement.[89] This means that civilians forfeit their protection for a limited period. There is thus a very narrow window when civilians committing DPH can be attacked which is even narrower in cyber operations due to their rapidity and the fact that it is not always easy to distinguish between the different stages or actions in a cyber operation or to understand their objectives.[90] In our opinion, the notion of combatancy based on membership adopted here can address this problem whereas for individual DPH, a more integrated approach to cyber operations should be taken.[91]

From the preceding discussion it transpires that unless the DPH tests are contextualized in the cyber domain, it will be difficult to operationalize the principle of distinction and apply it to CPK. These difficulties are compounded by the involvement of civilians in cyber operations and the fact that in a PKO civilian and military personnel operate side by side. The difficulties are equally serious when automatic cyber defence is used in dynamic and complex environments where participants perform interchangeable functions.

6. STRUCTURAL AND INSTITUTIONAL CHALLENGES TO CYBER-PEACEKEEPING

In this section we will expand on the structural and institutional challenges facing cyber-peacekeeping and discuss further the reforms that the introduction of CPK will require.

A serious and multilevel challenge CPK is facing is that of access to cyber technology. One aspect of this challenge concerns the UN and more specifically its access to cyber technology as well as the development of its own cyber infrastructure, resources and capabilities. If the UN develops its own cyber capabilities it will become less reliant on troop contributing countries (TCC) and minimize problems of interoperability. There are of course related costs but once cyber technologies are introduced, costs will be reduced. Another aspect of this challenge concerns the UN's relationship with the private sector and/or with its member States for access to material and human resources, technology and know-how. Engaging the private sector raises questions about costs but also about security and control. Relying on TCC which may have different capabilities and know-how, raises questions as to how they can be shared with the UN and other TCCs and how they can be made interoperable. A third aspect concerns the availability and adequacy of local cyber infrastructure. Without adequate or compatible cyber capabilities and infrastructure, a CPK cannot operate effectively unless the UN and/or TCC rely on or develop their own independent capabilities and infrastructure such as electricity, servers, copper wires, relay towers, computers, wifi, Bluetooth, etc. This is however time consuming and expensive and may not contribute to the long-term reconstruction of the State. To this, issues of cyber security should also be taken into account.

---

[89] Ibid., 65–8.

[90] For criticism of the ICRC approach see Bill Boothby, '"And for Such Time As": The Time Dimension to Direct Participation in Hostilities' (201) 42 *New York University of International Law and Politics* 741; Michael N Schmitt, 'The Status of Opposition Fighters in a Non-international Armed Conflict' (2012) 88 *International Law Studies* 119, 136. Also see *Law of War Manual* (n 65) para 5.8.4.

[91] Tsagourias and Morrison (n 70) 107–8, paras 4 and 5.

Another set of challenges refers to the fact that TCCs have different military doctrines and strategies concerning the use of cyber resources in situations of armed conflict. This may lead to fragmented mandates, complex operational rules, or lead to interference by national governments in decision-making. Related to this is also the question of determining which cyber technologies should be incorporated in a PKO and the purposes for which they should be used.

Another challenge relates to the question of how data or information collected through cyber means can be analysed, assessed, verified, contextualized and, generally, how they can be managed; by whom; and at what level. Also, what should be the degree of sharing and cooperation between TCCs, the mission HQ, and the different UN organs and departments in the management of information?[92] Related to this is the question of how local parties can be convinced that the data relied on for decision-making purposes are authentic and accurate. Convincing host States or other actors that the use of cyber technology will not serve unwarranted purposes or that cyber vulnerabilities or information will not be revealed is also a serious challenge.

Moving now to a different set of challenges, using cyber technology in PKO (especially antiquated one) may invite other actors, such as host States or armed groups, with more sophisticated technology, to launch cyber-attacks on PKO or spy upon them which can impede the effectiveness of the PKO. This leads to another challenge mentioned above, namely, how the UN can secure its cyber infrastructure and communication lines in particular in situations of armed conflict; who can provide this service; and whether the UN should partner with the private sector in this respect.

As noted in the previous section, the increasing use of civilians to operate cyber technology, will blur the distinction between civilians and combatants, increase the risk of attacks on peacekeepers and blur the applicable legal framework with serious legal and other consequences.

At the institutional level the introduction of CPK will require reconsideration of the peacekeeping doctrine, mandates, and rules of engagement, the tasks and purposes for which they are used, and how they are used. It would engender changes in the composition of the force with the introduction of cyber units/contingents or ICT experts as well as in the command structure with the introduction of cyber command centres. It will lead to the introduction of the concept of TechTCC (Technology Contributing Countries). SOFAs and MOU will also need to be renegotiated in order to take into account cyber technologies. Training will need to be adapted by providing pre-deployment training in the use of ICT[93] in order to ensure interoperability during the operation. It will finally require a review of the international law framework that applies to PKO in particular the application of IHL, IHRL and the DPH criteria in order to ensure compliance with international law but also accountability.

All the above represent challenges that policy makers and lawyers need to tackle by also taking into account the fact that incorporating cyber technologies in PKO secures greater efficiencies, allows the UN to become more independent from locals or TCC, and reflects developments in military and policing doctrine. That said, they should also recognise that, if all, or most, peacekeeping tasks are performed online, this may create disconnection with the local population and consequently affect the policy of winning hearts and minds and the

---

[92] HIPPO Report (n 13) paras 206 and 209; Olga Abilova and Alexandra Novosseloff, *Demystifying Intelligence in UN Peace Operations: Toward an Organizational Doctrine* (International Peace Institute, July 2016).

[93] UN Signals Academy https://operationalsupport.un.org/en/un-signals-academy.

feeling of security that physical presence provides. This will not only raise questions about the rationale of peacekeeping but also questions about the rationale of incorporating and using cyber technology in peacekeeping.

7. CONCLUSION

In the preceding sections we identified the peacekeeping tasks that can be cyberized, discussed what added-value this brings to peacekeeping and how they conform to the principles of consent, impartiality and use of force in self-defence. We also considered the legal framework that applies to the use of lethal force in cyber-peacekeeping. In this regard we considered the IHRL regulation of the use of lethal force and examined how the legal criteria of necessity, proportionality and precautions can apply thereto. We then considered the legal framework that applies to the use of force when cyber-peacekeepers operate in the course of an IAC or an NIAC. We said that the military personnel should be treated as combatants whereas the civilian personnel should be protected as civilians unless they commit DPH in which case they will forfeit their protection and be lawfully targeted for as long as their participation lasts. However, we identified a number of challenges in applying the IHRL, IHL and DPH criteria to CPK and for this reason we discussed ways of addressing these challenges. We then considered institutional and structural challenges that the introduction of CPK presents. Throughout this chapter we also highlighted the potential tensions between cyber-peacekeeping and the principles of impartiality and consent.

The main takeaway of this chapter is that the incorporation of cyber technologies in peacekeeping and cyber-peacekeeping itself present opportunities but they also pose certain legal, institutional and political challenges. For this reason, serious and detailed consideration is needed. Furthermore, the move to cyber-peacekeeping should be cognisant of the opportunities but also of the limitations it presents and would require a radical cultural shift since cyber-peacekeeping will change how the UN is conducting PKOs.

17. Some thoughts on cyber deterrence and public international law

Eric Myjer[1]

1. THE PROBLEM: INTRODUCTION

When it became clear that the Obama Administration was developing specific internal rules on the use of cyber weapons and drones, the *New York Times* reported on 3 February 2013[2] that a secret legal review on the use of cyber weapons had concluded that the US President has the broad power to order a pre-emptive strike 'if the US detects credible evidence of a major digital attack looming from abroad'. The article also said that in the next few weeks the US Administration would approve the first rules on how the military 'can defend, or retaliate against a major cyber-attack'. There was also reference to intelligence agencies carrying out searches of 'faraway computer networks' for 'signs of potential attacks on the US'. Furthermore, the article stressed that 'international law allows any country to defend itself from threats, and the US has applied that concept to conduct pre-emptive attacks'. It was finally noted that cyber weapons were so powerful that 'like nuclear weapons – they should only be unleashed on the direct orders of the president (the commander in chief)'. Not surprisingly, one of the subheadings of the article read: 'Cyber weaponry is perhaps the most complex arms race.' The impression that a cyber arms race is underway is supported by reports that a number of States are developing or have developed offensive cyber capabilities.[3] According to a 2014 report by the EastWest Institute, more than a dozen States were pursuing offensive cyber capabilities but this number has increased significantly. The report concluded that there

[1] The author would like to thank Jonathan Herbach for his comments on a previous draft of this chapter.

[2] David E Sanger and Thom Shanker, 'Broad powers seen for Obama in cyberstrikes', *New York Times* (3 February 2013) http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?pagewanted=all. See also (2013) 18 *J of Conflict & Security L* 1.

[3] That the US was acquiring an offensive cyber capacity appeared from the 'Presidential Policy Directive PPD-20' (US Cyber Operations Policy, 2012) https://fas.org/irp/offdocs/ppd/ppd-20-fs.pdf; See Glen Greenwald and Ewan MacAskill, 'Obama orders US to draw up overseas target list for cyber-attacks', *The Guardian* (7 June 2013) http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas. See for instance also: Zachary Keck, 'South Korea seeks cyber weapons to target North Korea's nukes', *The Diplomat* (21 February 2014) http://seclists.org/isn/2014/Feb/43 assessed 4 June 2014; Sue Halpern, How Cyber Weapons Are Changing the Landscape of Modern Warfare, *The New Yorker*, (18 July 2019) https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare; The U.S. Unleashes its Cyberweapons, *RealClearDefense* (8 July 2019) https://www.realcleardefense.com/articles/2019/07/08/the_us_unleashes_its_cyberweapons_114564.html.

is a militarisation of cyberspace 'which drives the urgent need to shield civilian critical infrastructure from peacetime cyber incidents, whether by accident or design'.[4]

Critical infrastructures[5] are under a constant threat of digital attacks. These attacks may be conducted by States or non-State actors to destabilise economic relations, steal information or for terrorist purposes. They may also aim to destabilise a State, or to disrupt an international organisation, or both. An example of the former is Russia's involvement in the US 2016 election.[6] An example of the latter is Russian involvement in the Brexit referendum in the United Kingdom (UK) and its support for the 'vote leave' campaign aimed at disrupting both the UK internally as well as the European Union's internal structure.[7] The assumption is that election inference in a constitutional democratic State aimed at influencing or disrupting that State's central democratic processes is equivalent to a breach of that State's critical infrastructure as generally understood, i.e., the effective functioning of government.

Interestingly, during the 2016 US election cycle, within the Obama administration there was talk of 'electoral security'[8] and of designating electoral infrastructure as 'critical infrastructure'.[9] This also points to a practical distinction that should be made between preventing a State's electoral infrastructure from manipulation by cyber means of a foreign State (or non-State actor), and by preventing a foreign State from using other means such as social media to influence the outcome of an election.[10]

It is, however, also possible that cyber-attacks take place for military purposes, such as where they support a conventional military attack. An example of a combined strike was

---

[4] Bruce W McConnell and Greg Austin, 'A measure of restraint in cyberspace, reducing risk to civilian nuclear assets' (East West Institute 2014) 10.

[5] See section 2 below.

[6] See for instance the clear conclusion by a committee of the US Senate: 'The Committee found that the Russian government engaged in an aggressive,multi faceted effort to influence, or attempt to influence, the outcome of the 2016 presidential election'; Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 US Election, Volume 5: Counterintelligence Threats and Vulnerabilities, US 116th Congress (1st session), Senate Report, 116-XX., released 18 August 2020, (I.(U) at v. On this report see also Mark Mazetti, 'A Republican-led Senate panel details the 2016 Trump campaign's Russian ties', *The New York Times* (18 August 2020); Reg Miller, Karoun Demirjian and Ellen Nakashima, 'Senate report details security risk posed by 2016 Trump campaign's Russia contacts', *The Washington Post* (19 August 2020). See on this also Peter W Singer and Emerson T Brooking, *Like War, The Weaponization of Social Media* (Eamon Dolan/Houghton Mifflin Harcourt 2018); David Shimer, *Rigged, America, Russia and One Hundred Years of Covert Electoral Interference* (William Collins 2020) and the sources quoted there. See also Kilovaty (Ch 5 of this Handbook).

[7] On Russian involvement see UK, *Intelligence and Security Committee of Parliament: Russia* (21 July 2020) https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl .

[8] Shimer (n 6) 182.

[9] Ibid., 183.

[10] The application/utilisation of social media to advance aggressive purposes more generally, even in combination with more 'traditional' kinetic uses of force, as part of an armed attack will not be dealt with here but has been forcefully and convincingly described by Singer and Brooking in their book *Like war* (n 6). On cybersecurity initiatives by the private sector, like Microsoft, for some form of control like a Digital Geneva Convention or the realized Cybersecurity Tech Accord 2018 (https://cybertechaccord.org/about/) and arms control (by States) and the Geneva Conventions, see Brad Smith and Carol Ann Browne, *Tools and Weapons*, *The promise and the peril of the digital age* (Penguin Press 2019) Chapter 7 (in particular 115 onwards).

Operation Orchard, which was the bombing raid by Israel on a nuclear reactor site at Dayr ez-Zor in North Syria in 2007, whereby the Israeli military combined electronic warfare with precision strikes.[11] 'It appears that the Israeli Air Force prepared for the main attack by taking out a single Syrian radar site at Tall al-Abuad close to the Turkish border.'[12] The other possibility would be, at least in theory, that a State (or non-State actor) would have the capability for a full-blown paralysing attack against another State by making use of its cyber capability.

Cyber weapons challenge the conflict and security lawyer, for many fundamental questions arise. For instance, what is the legal basis for a government hacking into 'faraway computer networks'? Is it just part of an open competition between the technologically most advanced States, or is it a variation on intelligence gathering by national technical means (NTMs) as in the past? When do these activities cross the threshold and become a threat or use of force? Can cyber operations ever be the equivalent to use of force? And when and how are States allowed to react? And does it make a difference whether it is a State or a non-State actor that is making the threat? Pre-emptive and preventive military action was the cornerstone of the *US National Security Strategy*, as presented by the Bush administration in September 2002.[13] Is this still the current US Security Strategy? Has there been a change in the general opinion among public international lawyers that there is no legal basis for a pre-emptive or preventive strike but only for self-defence against an armed attack (Article 51 UN Charter),[14] or when there is an imminent attack, or as Yoram Dinstein puts it, interceptive self-defence?[15] More generally, how are the self-defence criteria under the UN Charter, such as armed attack, proportionality and necessity, to be applied? Have new rules of customary law in this realm been developed?[16] But most importantly, do we have to conclude that a cyber-deterrent strategy[17] is being developed, either via self-defence or via retaliation? The mere mention of a possible preventive US reaction with extremely powerful cyber weapons against the possibility of a cyber threat brings back memories of the early deterrence discussions with regard to nuclear weapons.[18]

Under President Trump the discussion has continued: a National Cyber Strategy was published[19] and the White House implemented changes, repealing PPD-20 and replacing it with a new document, NSPM-13.[20] The intention of this new strategy was to reverse restraints

---

[11] Thomas Rid, *Cyber War Will Not Take Place* (OUP 2013) 42.

[12] Ibid.

[13] 'The National Security Strategy of the United States of America' (September 2002) www.state.gov/documents/organization/63562.pdf.

[14] See for instance 'Pre-Emptive action', Report by the Netherlands Government's Advisory Council on International Affairs (AIV) and the Advisory Committee on Issues of Public International Law (CAVV), No. 36, AIV/No 15, CAVV, July 2004 http://www.cavv-advies.nl/Publications.

[15] Yoram Dinstein, *War, Aggression and Self-Defence* (CUP 2001) 203–4.

[16] For a overview of these issues see Roscini and Focarelli (Chapters 14 and 15 respectively in this Handbook).

[17] 'Editorial: Deterrence Revisited?' (2013) 18 *J of Conflict & Security L.* 1.

[18] On the broader use of an information advantage already in 1996 see Joseph S Nye and William A Owens, 'America's Information Edge' (1996) 75 *Foreign Affairs* 20, 20 for instance where they remark: 'This information advantage can help deter or defeat traditional military threats at relatively low cost'.

[19] National Cyber Strategy of the United States of America (September 2018) https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[20] National Security Presidential Memoranda 13. See Jason Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace' (2019) 5 *J of Cybersecurity* 1, 3.

(i.e., Presidential authority) thereby enabling offensive cyber operations through the relevant departments. Regarding the deterrent purposes of this strategy, the then National Security Advisor John Bolton was quite explicit: 'We intend to, through both offensive and defensive cyber actions, create structures of deterrence that will reduce malign behavior in cyberspace.'[21] This led Healey to note a difference between a policymaker like John Bolton and the military under this strategy, explaining that '[p]olicymakers have not been as careful as the military in distinguishing between forward defense and deterrence'.[22] Healey goes on to explain that National Security 'Advisor John Bolton specifically tied the "revocation" of PPD-20 to cyber deterrence'.[23] Whatever the relevance of this distinction between the policymaker and the military, what stands is that deterrence is part of the current cyber strategy.[24]

This change in policy by the White House since the first edition of this Handbook does not, therefore, change the fundamental questions discussed in this chapter, for the principal aim is still to create structures of deterrence that will reduce malign behaviour in cyberspace. This chapter thus looks at the question of whether we see a cyber-deterrent strategy emerge and whether a parallel can be drawn between the deterrent strategies in the nuclear realm and such a strategy with regard to a possible cyber-attack by States in cyberspace and projected generic (preventive) replies by States to such threats. Furthermore, the chapter will deal with the question of whether such a cyber deterrent is allowed under public international law. This focus on cyber deterrence is State-oriented and this chapter therefore does not deal with non-State actors, and in this sense it is only concerned with part of the problem of possible offensive cyber operations.

Although it concerns the question of deterrence and cyber-security in general, the chapter will finally consider the possible implications regarding the cyber-security of nuclear assets like nuclear power plants. Does the discussion provide any insights into how to improve nuclear security?

Before discussing deterrence as such, the next section will briefly discuss the issue of cyber-security of critical infrastructures and in particular the security of nuclear assets from cyber threats.[25]

---

[21] The White House. *Transcript: White House Press briefing on national cyber strategy* (20 September 2018) https://news.grabien.com/making-transcript-white-house-press-briefing-national-cyber-strateg.

[22] According to Healey, 'both US Cyber Command and DoD [Department of Defence] treat the new strategy of forward defense as complimentary but distinct from cyber deterrence'; Jason Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace' (2019) 5 *J of Cybersecurity* 1, 3.

[23] Healey quoting Bolton from the same White House Press briefing: 'We have authorized offensive cyber operations […] not because we want more offensive operations in cyberspace, but precisely to create the structures of deterrence that will demonstrate to adversaries that the cost of their engaging in operations against us is higher than they want to bear'; ibid., 4.

[24] The National Cyber Strategy even refers to launching an International Cyber Deterrence Initiative with a coalition of like-minded States because '[t]he imposition of consequences will be more impactful and send a stronger message if it is carried out in concert with a broader coalition of like-minded states'; (n 19) 21.

[25] McConnell and Austin (n 4).

2. SECURITY AGAINST CYBER THREATS

(a) General

There are many ways in which the security of States could be threatened. On the one hand the *military security*[26] of a State could be endangered, which refers to security from interference by military means. The security of a State could for instance be threatened solely by military kinetic means or it could be done by a combination of military and cyber means, whereby for instance a cyber operation is aimed at disrupting the control by radars prior to a military attack on military targets. These security threats fall within the traditional realm of (collective) self-defence.

Of a different order would be a cyber-attack solely on civilian critical (information) infrastructures that are crucial to the operation of the State and whereby cyber-attacks could range from annoying disruptions of systems to chaos and enormous damage comparable to damage caused by an armed attack. This is about *cyber-security*, meaning security from interference by cyber means. In both these instances the central question is how to prevent such interference by either a military attack or by a comparable cyber operation, a cyber-attack for short. And what should be done to prevent such an attack, or in the case of an actual attack? It will be clear that there is a blurring of the lines between these two instances especially since the effects of such cyber-attacks could be comparable to those of an armed attack. After a general discussion this contribution will, in concluding, also look at cyber security of critical infrastructures of civil nuclear assets.

(b) Cybersecurity of Critical Infrastructures: The Objects and the Risks

Security in the cyber domain is a problem. Critical infrastructures are continuously being hacked by outsiders that either attempt to interrupt these information structures, or intend to inflict permanent damage.[27] It thereby concerns cyber-attacks on these structures.

The term critical infrastructure[28] is defined in this chapter in the same way as by the European Commission, namely, referring to those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious

---

[26] On the concept of military security and the ban on the use of force see Eric P J Myjer, 'The Law of Arms Control, Military Security and the Issues: An introduction' in Eric P J Myjer (ed), *Issues of Arms Control Law and the Chemical Weapons Convention* (Martinus Nijhoff 2001) 2–4.

[27] Barron-Lopez reports that 'of the roughly 200 cases of hacking attacks the cybersecurity team at the Department of Homeland Security handled in 2013, more than 40 percent were in the energy sector', which showed the energy sector to be the most vulnerable of the critical infrastructures to attacks. Laura Barron-Lopez, 'Cyber Threats Put Energy Sector on Red Alert', *The Hill* (12 June 2014) http://thehill.com/policy/technology/209116-cyber-threats-put-energy-sector-on-red-alert.

[28] See also Nicholas Tsagourias, 'Cyber Attacks, Self-defence and the Problem of Attribution' (2012) 17 *J of Conflict and Security L* 231, where the author refers to attacks on critical State infrastructure. According to the author, 'most definitions agree that certain services such as security, food, water, transportation, banking and finance, health and energy, governmental and public services constitute critical infrastructure'. See James C Mulvenon *et.al*., 'Addressing cyber instability' (Cyber Conflict Studies Association 2012) 339–63.

impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments.

Critical infrastructure includes services related to:

- energy installations and networks;
- communications and information technology;
- finance (banking, securities and investment);
- health care;
- food;
- water (dams, storage, treatment and networks);
- transport (airports, ports, intermodal facilities, railway and mass transit networks and traffic control systems);
- production, storage and transport of dangerous goods (e.g., chemical, biological, radiological and nuclear materials);
- government (e.g., critical services, facilities, information networks, assets and key national sites and monuments).[29]

Critical Information Infrastructure (CII) refers to the information systems, networks and data that support the safe or reliable operation of critical infrastructure.[30] The critical information infrastructures interconnect and affect their operations.[31]

Attacks on any of the critical infrastructures could lead to enormous damage. In particular, interference via cyber-attacks on production, storage and transport of dangerous goods (e.g., chemical, biological, radiological and nuclear materials) is extremely worrisome since it might lead to effects comparable to those of weapons of mass destruction. If one takes the example of radiological and nuclear materials the dangers that flow from the release of these materials in the environment are enormous, as illustrated by the case of the March 2011 Fukushima[32] incident in Japan. The Stuxnet[33] cyber-attack against Iran's nuclear enrichment program at Natanz shows that interfering with civilian nuclear assets is not a mere theoretical possibility, but has in fact occurred leading to approximately 1,000 centrifuges spinning out of control.[34] Even though it is assumed that the Natanz facility is merely one of the steps in the production of nuclear weapons by Iran, it demonstrates the vulnerability of nuclear-related facilities in general to cyber operations.

---

[29] Commission (EC), 'Critical Infrastructure Protection in the fight against terrorism' (communication) COM(2004) 702 final, 20 October 2004.

[30] McConnell and Austin (n 4) 10.

[31] UNGA Res 58/199 (30 January 2004) UN Doc A/RES/58/199 on the Creation of a global culture of cybersecurity and the protection of critical information infrastructures defines the relationship between critical infrastructures and the critical information infrastructures as follows:

> Noting the increasing links among most countries' critical infrastructures — such as those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health — and the critical information infrastructures that increasingly interconnect and affect their operations.

[32] See for instance 'Fukushima accident', *World Nuclear Association* (16 September 2014) http://www.world-nuclear.org/info/safety-and-security/safety-of-plants/fukushima-accident/.

[33] See for instance Rid (n 11) 43–5; McConnell and Austin (n 4) 10–1; Russell Buchan, 'Cyber Attacks: Unlawful uses of force or prohibited interventions?' (2012) 17 *J of Conflict & Security L* 211.

[34] McConnell and Austin (n 4). See also Rid (n 11) 43–6.

It is therefore vital to protect such infrastructures from outside interference to prevent possible large-scale damage to people and the environment. In other words, by reducing the risk to civilian nuclear assets, nuclear security will be improved. Compare in this context the Digital Agenda for Europe adopted by the European Commission.[35]

One particular element of the critical infrastructure that needs to be protected and bears close resemblance to the more 'classic' area of military security and arms control is the case of a nuclear power plant. There is a dual use dimension to this particular information infrastructure, for a cyber-attack resulting in interference with, or damage to, a nuclear power plant could turn it via the effects thereof into a (small-scale) nuclear weapon. In its report *A Measure of Restraint in Cyberspace*,[36] the EastWest Institute presents in no uncertain terms the urgency of acting to protect critical information infrastructures and in particular to reduce the risks to civilian nuclear assets.[37] The report warns of the militarisation of cyberspace which 'drives the urgent need to shield civilian critical infrastructure from peacetime cyber incidents, whether by accident or design'[38] and underscores the necessity for international agreements.

In what way could for instance the protection of a nuclear power plant be realised? Protection could of course be improved by making sure that such critical infrastructure is detached from the general cyber network (system) and has a standalone, solely facility-related cyber network. The report of the EastWest Institute mentions that a practical action may be 'to quarantine selected critical information infrastructure (CII) from cyber-attacks during peacetime as a measure of restraint'.[39]

With regard to the protection in peacetime of critical infrastructures, which are of a civilian nature, it needs to be stressed that in considering its protection in this contribution we will look at it from the perspective of deterrence and defence, which both concern *ius ad bellum* rules. More generally, of course, a State's 'classic' deterrence and defence by military means is always aimed at the preservation of a peacetime situation. With regard to cyber operations that may be threatening critical infrastructures, however, another focus could have been on the internet as primarily belonging to the sphere of economic and communications activity where, as quite rightly argued by Mary Ellen O'Connell, 'civil law enforcement officials have primary jurisdiction'.[40] This, however, is not the perspective taken in this chapter, which is driven by the debate on creeping militarisation of cyberspace.[41] The Cyber Conflict Studies Association (CCSA) refers to this approach as the 'warfare approach', which is characterised

---

[35] Commission (EC) 'A Digital Agenda for Europe' (Communication) COM(2010)245 final (19 May 2010).

[36] McConnell and Austin (n 4).

[37] See also the Report of Working Group 2 –Managing Cyber Threat- to the Nuclear Industry Summit 2014, which was held prior to the 2014 Nuclear Security Summit in The Hague.

[38] McConnell and Austin (n 4) 10.

[39] Ibid.

[40] Mary Ellen O'Connell, 'Cyber Security Without Cyber War' (2012) 17 *J of Conflict & Security L* 188.

[41] See Introduction.

by a militarised outlook on cyber conflict.[42] Interesting in this respect is Thomas Rid's remarks that '[w]hat has been militarized is the debate about cyberspace'.[43]

The approach taken in this chapter does not mean that all the premises associated with those[44] who draw Cold War parallels with regard to cyber security are automatically accepted. An important point to take into consideration is Rid's argument that cyberspace is not a fifth domain of warfare for it 'is not a separate domain of military activity',[45] which led him to conclude that 'the debate on national security and defence would be well served if debating war was cut back to the time tested four domains'.[46]

One of the questions under consideration in this chapter is how do defensive and offensive cyber operations fit in, like those mentioned earlier as in the case of the US,[47] when considering the protection of critical (information) infrastructures? More specifically, could they be regarded as part of a cyber-deterrent strategy, and is such a deterrent strategy allowed for under public international law?

3. PROTECTION VIA DETERRENCE: THE CONCEPT OF DETERRENCE AND ITS CENTRAL ELEMENTS[48]

What deterrence basically comes down to is making clear to any potential opponent that if you dare to attack me you may expect, at a minimum, a reply in kind, that will be devastating to your potential. It may also include the message that even if attacked my capacity to make such a reply will be preserved by a guaranteed second strike, so a first strike will not give an advantage. Deterrence in international relations therefore is about discouraging a potential aggressor by projecting the reply that will follow in case of an attack. It is about preventing an attack by making known to any possible aggressor such a substantial reply that it will forsake such an attack. Morgan refers to 'threats to inflict unacceptable harm on the attacker'. In his words this can be done by 'a stout defense' or 'through retaliation'.[49] When it concerns the projection of

---

[42] Mulvenon *et.al.* (n 28) 290. Other approaches discussed in their report are the technical approach, the criminal approach and emerging approaches like public health, environmental and irregular warfare (283–onwards).

[43] '[I]f militarizing cyberspace means establishing robust cyber defences, than cyberspace has not been militarized. What has been militarized is the debate about cyberspace'; Rid (n 11) 174.

[44] On participants in the cyber debate who make comparisons with the Cold War and nuclear weapons, see ibid., 170.

[45] Ibid., 166.

[46] Ibid. The four domains refer to land, sea, air and space.

[47] See sources mentioned in n 3.

[48] See on deterrence in general Eric PJ Myjer, *Militaire Veiligheid door Afschrikking, verdediging en het geweldverbod in het Handvest van de Verenigde Naties* (Military Security via Deterrence, Defence and the ban on the use of force in the United Nations Charter) (in Dutch) (Kluwer 1980).

[49] In international politics:

> deterrence refers to efforts to avoid being deliberately attacked by using threats to inflict unacceptable harm on the attacker in response. The threatened harm can be inflicted by a stout *defense*, frustrating the attack or making it too costly to continue, or by turning its success into a pyrrhic victory. Or it can be inflicted through *retaliation*. (And through a combination of the two).

Patrick M Morgan, 'Applicability of traditional deterrence concepts and theory to the cyber realm' in National Research Council, 'Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy' (The National Academies Press 2010) 55. See also

a credible defence in case of attack nothing is wrong, for each State is entitled to defend itself under both Article 51 UN Charter and customary law. An example of this is a statement by the Secretary General of NATO who, in the context of the Ukraine political standoff, remarked: 'Today, we will show our steadfast commitment to NATO's collective defence. Defence starts with deterrence.' The Statement went on to say: 'So we will take the necessary steps to make it clear to the world that no threat against NATO Allies will succeed.'[50] This case of deterrence via the projection of defence is about self-defence and it is not therefore a forbidden threat to use force under Article 2(4) UN Charter, although the distinction sometimes may be rather subtle. Of course, such self-defence action needs to answer to principles like necessity, proportionality and immediacy. A totally different case, however, is threatening retaliation by the projection of a blatant use of force, meaning use of force breaching these principles. Deterrence via retaliation is highly questionable from the point of view of public international law. This, however, did not prevent nuclear weapon States from adopting such a strategy. Even since the end of the Cold War this nuclear-deterrence strategy has been maintained and is still being applied.[51] The projected reply in case of an attack by nuclear means is through retaliation by nuclear means.

Given that in parallel with a defensive cyber capacity a so-called offensive cyber capacity is also being developed,[52] the question is whether this might lead to a similar deterrent strategy in the cyber area, namely cyber deterrence, which would not only deter with the projection of a credible defensive capability and a credible will to apply it in case of an attack (which is not possible in the case of nuclear deterrence, as will be explained) but also via the projection of retaliation via offensive means? To begin with: would it be possible to retaliate against a particular (specific) cyber aggressor? Could the attacker be identified quickly and without any reasonable doubt? And more generally, would it be a viable and acceptable strategy? And if so, would it be allowed for under public international law, or is it a forbidden threat with regard to the use of force?

---

his early theoretical study on deterrence: Patrick M Morgan, *Deterrence a Conceptual Analysis,* Sage Library of Social Research, Volume 40, 1977. Libicky chooses to equate deterrence with retaliation and not also with defence. See Martin C Libicky, *Cyberdeterence and Cyberwar* (RAND Corporation 2009) 7:

> If deterrence is anything that dissuades an attack, it is usually said to have two components: deterrence by denial (the ability to frustrate the attacks) and deterrence by punishment (the threat of retaliation). For purposes of concision, the use of deterrence in this work refers to deterrence by punishment. This is not to deny that defense has no role to play – indeed, the argument here is that it does play the greater role and rightfully so. Our discussion of deterrence (by punishment) asks whether it should be added to defense (deterrence by denial). Also, […] deterrence by denial and deterrence by punishment are synergistic with one another in some ways. Nevertheless, from this point on, deterrence refers to deterrence by punishment; the rest is defense.

See for a different approach to cyber deterrence Eric T Jensen, 'Cyber Deterrence' (2012) 26 *Emory Intl L Rev* 773.

[50] 'Statement by NATO Secretary General Anders Fogh Rasmussen at the start of the NATO Foreign Affaires Meeting' (NATO, 1 April 2014).

[51] Interestingly before the Russian usurpation of the Crimea few policymakers in the West were willing to face this fact.

[52] 'More than a dozen states are now pursuing offensive cyber capabilities'; McConnell and Austin (n 4) 10.

Before attempting to answer these questions, the next section will first give a short description of how nuclear deterrence developed with its projection of massive devastation via retaliation with offensive means, which ultimately leads to Mutual Assured Destruction (MAD).

4. NUCLEAR DETERRENCE

Deterring a potential aggressor by showing a credible capacity for defence or retaliation and a credible will to apply it in case of an attack as a strategy has existed for a very long time. Given that defence against nuclear weapons is not possible, nuclear deterrence with retaliation as its core element started when, after World War II, the US was still the sole possessor of nuclear weapons.

It later became known as the strategy of massive retaliation, in which the US strategic retaliatory capacity was central. Its prime aim was to deter Soviet aggression. This strategy originated, to a large extent, from budgetary constraints that made it difficult to build up US conventional forces to outweigh what was assumed to be the superior Soviet conventional forces. In his famous speech in January 1954 to the Council on Foreign Relations, the US Foreign Minister John Foster Dulles presented the strategy of deterrence and the role of nuclear weapons. A crucial element in his so-called massive retaliation speech was where he remarked: 'The way to deter aggression is for the free community to be willing and able to respond vigorously at places and with means of its own choosing.'[53] It was, in other words, about organising maximum security at minimal costs. Central to this strategy is deterrence via retaliation not via defence. This strategy is also important because it can be regarded as the first systematic theory of deterrence in the age of the Cold War.[54]

Although the Dulles speech took place four years after the first explosion of a Soviet atom bomb, and a few months after that of a thermo-nuclear weapon, it would still take some time before the possibility that the Soviet Union could answer with similar means was taken into consideration. That, however, changed after it became apparent that the Soviet Union had also developed the capability to deliver nuclear weapons in reply. This introduced the so-called balance of terror that would, in the end, lead via the concept of mutual deterrence to that of mutual assured destruction (MAD), which still forms part of present-day security strategy with regard to nuclear weapons in which deterrence plays a predominant role. Two elements were crucial in this strategy. The first is that a nuclear attack would have devastating consequences against which a proportional defence would be impossible. This made it essential to threaten with retaliation in kind in case of a nuclear attack (a so-called first strike). For this to be a credible threat in reply it was essential that such retaliation in a second strike was possible. This second strike potential was realised via the so called Triad, a combination of nuclear weapons on submarines, airplanes and on land-based missiles, whereby an attacker would never be able to make a first strike whereby the full nuclear inventory of the opponent would be annihilated (destroyed). Next to that a 'watertight' defensive shield against incoming missiles was techni-

---

[53] John F Dulles, 'The Evolution of Foreign Policy' (1954) 30 *Department of State Bulletin*. See Bernard Brodie, *Strategy in the Missile Age* (Princeton University Press 1971) 241. See also three months later John F Dulles, 'Policy for Security and Peace' (1945) 32 *Foreign Affairs* 353.

[54] Alexander L George and Richard Smoke, *Deterrence in American Foreign Policy, Theory and Practice* (Columbia University Press 1974) 27. See also Myjer (n 48) 49.

cally not possible, although in the early 1980s research into this possibility was given a boost under Ronald Reagan with the Strategic Defense Initiative or so called Star War's strategy. This led to accepting mutual vulnerability of which the ABM (anti-ballistic missile) treaty[55] was an expression.

At least at the strategic level, this doctrine still operates and answers the basic idea of deterrence, namely, deterring a potential aggressor by mirroring the nuclear reply that will follow in case of an attack. Interestingly, this strategy survived the Cold War and is still the current strategy with regard to nuclear weapons.[56] This is still the case in spite of the fact that, in 2002, George W Bush withdrew the US from the ABM Treaty in order to be able to further develop and eventually install missile shields, thereby bringing into question the US's willingness to accept the premise of the nuclear-deterrent strategy, that is, to remain vulnerable to a possible nuclear attack. Since to this day no effective nuclear shield has been developed, there is still this mutual vulnerability. What is different, however, is that nowadays there are more nuclear weapons and nuclear weapons States than in the 1950s, with India, Pakistan, Israel and North Korea now also nuclear weapon States.

On the question of whether this strategy is in conformity with public international law, the International Court of Justice (ICJ) gave its ambivalent advisory opinion (see below).

5. NUCLEAR DETERRENCE AND PUBLIC INTERNATIONAL LAW: THE NUCLEAR WEAPONS CASE

The only time the ICJ addressed the concept of deterrence was when it was raised in the *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) (1996).[57] Yet, the Court did not pronounce on this matter directly:

> 67. The Court does not intend to pronounce here upon the practice known as the 'policy of deterrence'. It notes that it is a fact that a number of States adhered to that practice during the greater part of the Cold War and continue to adhere to it […][58]

The argument about deterrence was raised in the context of the question of whether there existed a rule of customary international law prohibiting the threat or use of nuclear weapons as such. According to the ICJ, on the one hand States:

> which hold the view that the use of nuclear weapons is illegal have endeavoured to demonstrate the existence of a customary rule prohibiting this use. They refer to a consistent practice of non-utilization

---

[55] Treaty between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Ant-Ballistic Missile Systems (26 May 1972).

[56] Whether there still is a situation of MAD or whether the US is developing nuclear primacy was raised by Keir A Lieber and Daryl G Press, 'The Rise of U.S. Nuclear Primacy' (2006) 85 *Foreign Affairs* and further developed in Keir A Lieber and Daryl G Press, 'The End of MAD? The nuclear dimension of U.S. primacy' (2006) 30 *Intl Security* 7. The Essay in Foreign Affairs led to a response by a number of authors denying the Lieber and Press thesis and stressing that there still is a MAD situation. See Peter C Flory, 'Nuclear Exchange: Does Washington really have (or want) nuclear primacy? (2006) 85 *Foreign Affairs* 149.

[57] *Legality of the threat or use of nuclear weapons* (Advisory opinion) [1996] ICJ Rep 226, 229.

[58] Ibid., para 67.

> of nuclear weapons by States since 1945 and they would see in that practice the expression of an *opinio iuris* on the part of those who possess such weapons.[59]

On the other hand, there were some States:

> which assert the legality of the threat and use of nuclear weapons in certain circumstances, invoked the doctrine and practice of deterrence in support of their argument. They recall that they have always, in concert with certain other States, *reserved the right to use those weapons in the exercise of the right to self-defence against an armed attack threatening their vital interests*. In their view, if nuclear weapons have not been used since 1945, it is not on account of an existing or nascent custom but merely because circumstances that might justify their use have fortunately not arisen.[60]

Against the background of these arguments the ICJ decided not to pronounce on the 'policy of deterrence':

> It notes that it is a fact that a number of States adhered to that practice during the greater part of the Cold War and continue to adhere to it. Furthermore, the Members of the international community are profoundly divided on the matter of whether non-recourse to nuclear weapons over the past fifty years constitutes the expression of an *opinio iuris*. Under these circumstances the Court does not consider itself able to find that there is such *opinio iuris*.[61]

The Court, however, made clear that the rules of *ius ad bellum* and of *ius in bello* (the humanitarian law of armed conflict) apply to nuclear weapons, including the customary law principles of proportionality and necessity:

> Nevertheless the Court considers that it does not have sufficient elements to enable it to conclude with certainty that the use of nuclear weapons would necessarily be at variance with the principles and rules of law applicable in armed conflict in any circumstance.[62]

Also, the 'fundamental right of every State to survival, and thus its right to resort to self-defence, in accordance with Article 51 of the Charter, when its survival is at stake',[63] was taken into consideration, as was the fact that it could not ignore 'the practice referred to as "policy of deterrence"'.[64] The Court then concluded, by seven votes to seven with the President's deciding vote, and what widely is referred to as a *non-liquet*,[65] that it is 'led to observe that it cannot reach a definitive conclusion as to the legality or illegality of the use of nuclear weapons by a State in an extreme circumstance of self-defence, in which its very survival would be at stake'.[66] Given that deterrence is about projecting a reply in case of attack, with this conclusion regarding the use of nuclear weapons in self-defence no definitive conclusion can be drawn as

---

[59] Ibid., para 65.
[60] Ibid., para 66 (emphasis added).
[61] Ibid., para 67.
[62] Ibid., para 95.
[63] Ibid., para 96.
[64] Ibid.
[65] See on this for instance Ige F Dekker and Wouter G Werner, 'The Completeness of International Law and Hamlet's Dilemma' (1999) 68 *Nordic J of Intl L* 225.
[66] *Legality of the threat or use of nuclear weapons* (n 57) para 97. See also the lengthy dissenting opinion of Judge Weermantry, and in particular on deterrence (VII- pp. 76–9), where he discusses in particular the concept of deterrence.

to whether the projection of this 'self-defence by nuclear weapons' is legitimate self-defence or a forbidden threat to use force under Article 2(4) UN Charter. In other words, it leaves open the question regarding the legitimacy of nuclear deterrence.

6. CYBER DETERRENCE

This section looks at the question of whether a cyber-deterrent strategy comparable to the nuclear-deterrent strategy is possible. The reason to make such a comparison is because of some common characteristics of the way the US announces its nuclear-deterrent strategy and its cyber strategy, namely, the prevention of threats of vital interests via the projection of indiscriminate offensive nuclear means against nuclear attacks or via offensive cyber means in the case of a cyber-attack.

The reason for trying to assess whether we are witnessing the development of a comparable strategy of deterrence in cyberspace is not because cyber-attacks can be one-on-one compared with attacks by nuclear weapons. The consequences of cyber-attacks will have to be measured individually. When looking at some of the central elements of nuclear deterrence the conclusion is clear that cyber deterrence (deterring cyber-attacks with cyber means) by projection of a cyber threat comparable to the threat under nuclear deterrence is – at present – technically not possible. The crucial difference between nuclear deterrence and cyber deterrence is that the deterrent threat in the former case is retaliation, and in the latter case might be either defence or retaliation. This is the case in spite of the suggestion by the ICJ in the *Nuclear Weapons* opinion that this might be qualified as a defensive option in cases where the survival of a State is at stake.[67]

In its report *Addressing Cyber Instability*, the CCSA[68] examined to what extent nuclear deterrence and cyber deterrence can be compared. It goes back to the basics of the strategies on deterrence of theorists like Thomas Shelling or Jerome Kahn, although the latter author is not explicitly referred to. It concludes then that 'the current strategic cyber environment is structurally unstable, marked by an inability to establish credible deterrence [and strong incentives to strike pre-emptively]'.[69] To a large degree the system of nuclear deterrence is transparent insofar as the effects of nuclear weapons are known; we know who are the nuclear weapon States and what is their nuclear capacity; and we know where their nuclear sites are located because of various monitoring systems (including, *inter alia*, national technical means like satellites). And given the triad of nuclear launch possibilities, it is generally accepted that a guaranteed second strike exists. In that sense, nuclear deterrence refers to deterrence as formulated by the US Strategic Command:

---

[67] Ibid:
It follows from the above-mentioned requirements that the threat or use of nuclear weapons would generally be contrary to the rules of international law applicable in armed conflict, and in particular the principles and rules of humanitarian law. However, in view of the current state of international law, and of the elements of fact at its disposal, the Court cannot conclude definitively whether the threat or use of nuclear weapons would be lawful or unlawful in an extreme circumstance of self-defence, in which the very survival of a State would be at stake.
(seven votes to seven, by the President's casting vote).

[68] Mulvenon and others (n 28).

[69] Ibid. 31.

> Deterrence [seeks to] convince adversaries not to take actions that threaten U.S. vital interests by means of decisive influence over their decision-making. Decisive influence is achieved by credible threatening to deny benefits and/or impose costs, while encouraging restraint by convincing the actor that restraint will result in an acceptable outcome.[70]

When applying some of these criteria to the technical possibility of a convincing cyber-deterrent threat, either via retaliation or via defence, some uncertainties stand out.[71] To start with it is not clear who the potential adversaries are. They may be States or non-State actors, and given the broad availability of cyber means they may be innumerable. And in case of a cyber-attack it may be very difficult, if not impossible, to attribute[72] the attack and therefore impose the projected costs. And how do we know for sure that it is a case of a cyber-attack and not a mere case of (economic) espionage? Also, the cyber network may be unstable, because the same cyber network that is under attack may need to be used for the execution of the retaliatory or defensive cyber deterrent threat and the system itself might not be able to transmit the reply.[73] And if the deterrent threat of applying a so-called (retaliatory) offensive cyber capacity would be executed, might this not lead to total destruction, for instance, as a result of completely infecting cyberspace?[74] Might it then not 'blow up in the face' of the State reacting with a retaliatory strike since it is the same cyberspace that attacker and attacked are making use of? If so, it would be a form of cyber retaliation comparable to retaliation by nuclear weapons and its all-encompassing consequences. And given that the system might break down, can a guaranteed second strike capability be projected?

That nuclear deterrence and cyber deterrence are different in character was also made clear in a report from the Committee on Deterring Cyberattacks:

> […] But it is an entirely open question whether cyber deterrence is a viable strategy. Although nuclear weapons and cyber weapons share one key characteristic (the superiority of offence over defence), they differ in many other key characteristics […] What the discussion below [in the report] will suggest is that nuclear deterrence and cyber deterrence do raise many of the same questions, but that the answers to these questions are quite different in the cyber context than in the nuclear context.[75]

The conclusion therefore appears clear that a convincing strategy of cyber deterrence with the projection of a convincing retaliatory cyber threat, at present at least, is not possible.

---

[70] US Department of Defense, 'Deterrence Operations: Joint Operating Concept' (Version 2.0 December 2006) http://www.dtic.mil/futurejointwarfare/concepts/do_joc_v20.doc as quoted in 'Reprinted Letter Report from the Committee on Deterring Cyberattacks' in National Research Council (n 49) 350.

[71] See more details in National Research Council (n 49) 350–9.

[72] On the difficulties of attribution see Tsagourias (n 28) 233. Also see Nicholas Tsagourias and Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges' (2020) 31 *Eeuropean Journal of International Law* 941. Rid (n 11) 139–62. However, advances with regard to attribution have been made, the cases of Russian election interference as discussed in the introduction being a case in point.

[73] This may not affect the passive defence of the information structures, but at least the active defence. This would put a 'premium' on a first strike, or even be an incentive to use kinetic force in reply.

[74] This follows from the very interconnectivity of cyberspace, which is one of its great assets, but at the same time also constitutes its greatest vulnerability.

[75] US Department of Defense (n 70); Libicky (n 49) iii: 'Thus, deterrence and warfighting tenets established in other media do not necessarily translate reliably into cyberspace.' See also Ch III, 39–74.

However, deterrence is not solely realised via the projection of a retaliatory strike. It could also be realised via the projection of, in terms of Morgan, a robust[76] self-defence of both a passive and an active nature. In relation to the discussion referred to in the introduction of this chapter – that the US is acquiring an offensive cyber capacity – the suggestion is that such means are exclusively of an offensive character. Although of course it concerns questions of specific cyber technology, there also appears to be an element of semantics. For when a so-called offensive cyber capacity would be used as a means of cyber deterrence via the threat of retaliation it would not work for reasons discussed above. However, could not the same cyber technology be used for both offensive and defensive purposes?

In other words, when one considers the application of a restricted use of this so-called offensive cyber capacity, like the application of traditional military means, which could both be used offensively or defensively, the logical question appears to be whether it is possible to make a similar distinction between the way a digital capacity is used (applied), namely either offensively or defensively, or is an offensive digital capacity by definition different in character from a defensive digital capacity? If the former is the case, then it would come down to the way cyber power is being applied and not what label has been attached to the specific cyber capacity. Would it in that case not be better to speak of a cyber capacity that can be applied either offensively or defensively? The different categories that one finds in the leaked Presidential Policy Directive/PPD-20 of October 2012[77] in that respect are intriguing for, besides *Network Defense*,[78] it refers to *Defensive Cyber Effects Operations (DCEO)*[79] and to *Offensive Cyber Effects Operations*.[80] Both categories are intended to produce effects outside US Government networks. The defensive operation does so 'for the purpose of defending or protecting against imminent threats or on-going attacks or malicious cyber activity against U.S. national interest from inside or outside cyberspace'. The offensive operations appear not to be related to the defensive operation's purpose, but seem to be open ended since it merely refers to 'to enable or produce effects outside United States Government networks'.

Deterrence by the projection of a defence that can convincingly deny a potential attacker (any) benefits either actively or passively therefore appears a more viable deterrent strategy. Although a number of the same uncertainties, as discussed above, with regard to the techni-

---

[76] I regard this qualification as indicating a serious and optimal self-defence, taking into consideration the applicable principles of public international law.

[77] Presidential Policy Directive PPD-20 (n 3); Greenwald and MacAskill (n 3).

[78] 'Programs, activities, and the use of tools necessary to facilitate them… Network defense does not involve or require accessing or conducting activities on computers, networks, or information or communications systems without authorization from the owners or exceeding access authorized by the owners.' Presidential Policy Directive PPD-20 (n 3) 2.

[79] Defensive Cyber Effects Operations (DCEO):
Operations en related programmes or activities – other than network defence or cyber collection –conducted by or on behalf of the US Government, in or through cyberspace, that *are intended* to enable or produce cyber effects outside US Government networks *for the purpose of defending* or protecting against imminent threats or ongoing attacks or malicious cyber activity against US national interests from inside or outside cyberspace.
ibid., 3 [emphasis added].

[80] 'Offensive Cyber Effects Operations: Operations and related programmes or activities – other than network defense, cyber collection, or DCEO – conducted by or on behalf of the US Government, in or through cyberspace, *that are intended to enable or produce cyber effects outside the US Government networks*;' ibid., 3 [emphasis added].

cal possibility of a reply to a cyber-attack apply, such a more restricted approach aimed at an optimal defence appears more realistic and therefore more convincing. On the balance between defence and offense in the context of cyber-attacks, Rid comes down on the defence side. 'Cyber-attack, proponents of the offense-dominance school argue, increases the attacker's opportunities and the amount of damage to be done while decreasing the risks (sending special code is easier than sending Special Forces).'[81] However, Rid convincingly makes the case that 'it appears that cyberspace does not favour the offense, but actually has advantages for the defence in stock'.[82] Furthermore, deterrence by the projection of defence appears to align with a State's inherent right to self-defence in case of an armed attack and would be therefore in accordance with public international law. The compatibility of cyber deterrence with public international law is looked at in the next section.

7. CYBER DETERRENCE AND PUBLIC INTERNATIONAL LAW

Cyber deterrence with the threat of a retaliatory use of force could in most cases not be attacker-specific and would not answer the demands of public international law since the projected threat in case of an attack is a use of force that by definition would neglect the applicable criteria of proportionality and necessity. Also, such a strategy would not take into account the distinction between a use of force and an armed attack, as well as the further self-defence criteria and the law of armed conflict criteria. Nuclear deterrence cannot be taken as a precedent for that is a special case, where the ICJ has apparently taken the political realities ('practices') into consideration. Nuclear deterrence is about deterring via a threat of a retaliatory strike, which would lead to MAD. Such a strategy in fact comes down to self-destruction and not to actual self-defence. Nuclear deterrence works as long as there is no nuclear attack. The assumption, then, is that no nuclear exchange has taken place as yet because of the deterrent threat, but this cannot be proven. A careful reading of the ICJ advisory opinion provides all the arguments for why – from a legal point of view – this strategy is highly questionable, but that it is embedded in political reality. The political reality is that nuclear deterrence is central to the superpowers' strategy, whereby the mere possession of large quantities of nuclear weapons already contributes to nuclear deterrence and nuclear weapons so far have not been used (except for Hiroshima and Nagasaki). This led the ICJ to the conclusion that use of nuclear weapons might be legal when used as a measure of last resort in cases where the survival of that State would be at stake. (This conclusion in itself has strengthened nuclear deterrent strategy!). Although the ICJ did not formulate the political reality argument in those terms, this is what its advisory opinion came down to.

Although a cyber-attack is different from a kinetic attack, it may still amount to a use of force that is forbidden. The rules of the UN Charter relating to the threat and use of force 'apply to any use of force, regardless of the weapons employed' as the ICJ pronounced in the *Nuclear Weapons Case*.[83] In his report on *Cyber Operations in International Law*, Michael

---

[81] Rid (n 11).

[82] Ibid., 167–9.

[83] *Legality of the threat or use of nuclear weapons* (n 57) para 39. On the use of force in cyberspace see Roscini (Ch 14 of this Handbook).

Schmitt convincingly explains how cyber operations may fall under force as meant in Article 2(4) UN Charter.[84] When, then, does a cyber operation that does not inflict kinetic harm on a victim State become a use of force? According to the Tallinn Manual: 'A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.'[85] For Schmitt, 'the threshold for use of force therefore lies somewhere along the continuum between economic and political coercion on the one hand and acts which cause physical harm on the other'.[86] Earlier Schmitt identified seven factors that are likely to be taken into account when assessing whether a cyber operation could be seen as a use of force, namely, severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy and responsibility.[87] But even if a cyber operation can be classified as a clear use of force, this leaves us to consider two issues. First, Article 2(4) UN Charter prohibits the *threat* of force as well as the use of force. Second, there is a gap between Article 2(4) and Article 51 UN Charter since not all uses of force allow for forceful protective measures in self-defence; rather, it is only those uses of force that rise to the level of an armed attack that engage the right of self-defence.

The point of departure therefore is that under public international law both the threat and use of force in international relations are forbidden, and that the only exceptions to this rule are the use of force in self-defence or where force is mandated by the Security Council under Chapter VII in case of a threat to the peace, breach of the peace or act of aggression. Self-defence may only take place in case of an armed attack, as described in Article 51 UN Charter. These are the familiar rules in case of a traditional military (kinetic) armed attack and the possibility of a legitimate military reply. But how can we determine whether a cyber -attack amounts to the equivalent of an armed attack?

According to the Tallinn Manual, a cyber operation can be equated with a use of force when its scale and effects are comparable.[88] In order to identify cyber operations that could be described as uses of force (and based primarily on Schmitt's criteria), the Tallinn Manual mentions the following factors that could be taken into consideration: severity, immediacy, directness, invasiveness, State involvement, presumptive legality measurability of effects and military character.[89] Use of force, however, is not identical to an armed attack. The distinction between a use of force in Article 2(4) and an armed attack in Article 51 is apparent from the Charter. It means that to be able to act in self-defence the cyber operation in scale and effects needs to be equal to an armed attack.

---

[84] Michael N Schmitt, 'Cyber Operations in International Law: The use of force, collective security, self-defence, and armed conflicts' in National Research Council (n 49) 153–60. See further Roscini (Ch 14 of this Handbook).

[85] Michael N Schmitt (ed), *Tallinn Manual 2.0 on The International Law Applicable to Cyber Operations* (CUP 2017) (Tallinn Manual) Rule 69 (definition of use of force) at 330. The Tallinn Manual, which is the result of a lengthy research project by a group of international experts, at this moment can be regarded as the most authoritative publication on issues of cyber war and public international law. See also Michael N Schmitt, 'International Law in Cyberspace: The Koh speech and Tallinn Manual juxtaposed' (2012) 54 *Harvard Intl L J* 13.

[86] Schmitt (n 84) 155.

[87] Ibid. 155–6.

[88] Tallinn Manual (n 85) 330. On cyber-attacks and self-defence see Focarelli (Ch 15 of this Handbook).

[89] Tallinn Manual (n 85) Rule 69, paras 9 and 10.

In order to establish that a cyber operation amounts to an armed attack under Article 51 UN Charter, it is necessary to not only apply Schmitt's seven criteria but also to decide whether the consequence of the application of a cyber operation would be equal to a 'traditional' armed attack. Schmitt takes a consequence-based approach. 'Applying the consequence based approach, armed attack must also be understood in terms of the effects typically associated with the terms 'armed'. The essence of an 'armed' operation is the causation, or risk thereof, of death of or injury to persons or damage to or destruction of property and other tangible objects',[90] like critical infrastructure.[91] When the conclusion is that the cyber operation amounts to an armed attack under Article 51 UN Charter, self-defence is allowed. I share Schmitt's opinion that such use of force in self-defence can involve cyber as well as kinetic means.[92] This use of force would need to be in accordance with the principles of necessity, proportionality[93] and immediacy;[94] also the Security Council would need to be informed. Projecting the intention to make use of the right of self-defence in case of a cyber-attack amounting to an armed attack would be a lawful threat to use force as the ICJ made clear in the *Nuclear Weapons Case*: 'if it is to be lawful, the declared readiness of a State to use force must be a use of force that is in conformity with the Charter'.[95] This can be seen as deterrence via self-defence.

With the conclusion that a cyber-attack may amount to an armed attack, from the perspective of deterrence this would logically lead to a more refined model, whereby the deterrent threat of defence (denying of the gains sought by the cyber attacker) could be done either by cyber means, by a combination of cyber and kinetic means or even solely by kinetic means. Opting for a more comprehensive deterrence mode risks leading to a definitive militarisation of cyberspace. It could, for instance, be the option for a State that does not have advanced cyber means at its disposal, but is strong in traditional military (kinetic) hardware.

Furthermore, it is debated as to whether a State can only take self-defence action where an armed attack has actually materialised, or whether it may also defend itself in case of an imminent attack.[96] An imminent armed attack would, in my opinion, have to be one that is under way, in other words an irreversible attack. This position is close to that taken by Dinstein

---

[90] Schmitt (n 84) 163.

[91] See also Tsagourias (n 28) 231.

[92] Schmitt (n 84) 167.

[93] 'The submission of the exercise of the right to self-defence to the conditions of necessity and proportionality is a rule of customary international law.' As the Court stated in the case concerning *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* [1986] ICJ Rep 14, para 176): 'there is a specific rule whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it, a rule well established in customary international law'. 'This dual condition applies equally to art 51 of the UN Charter, whatever the means of force employed': *Legality of the threat or use of nuclear weapons* (n 57) para 41. See also Judith Gardam, *Necessity, Proportionality and the Use of Force by States* (CUP 2004).

[94] This is a different criterion than the immediacy principle of Schmitt. Here it refers to the reaction time and the length of the self-defence operation. Compare also Dinstein (n 15) 233–4. Schmitt formulates an immediacy principle as one of the principles to decide whether a cyber operation amounted to a use of force, namely: 'The sooner consequence1s manifest, the less opportunity States have to seek peaceful accommodation of a dispute or to otherwise forestall their harmful effects. Therefore, States harbour a greater concern about immediate consequence than those which are delayed or build slowly over time': Schmitt (n 84) 156.

[95] *Legality of the threat or use of nuclear weapons* (n 57) para 47.

[96] See Dinstein (n 15) 203–onwards.

who refers to interceptive self-defence.[97] Where the concept of imminence in the traditional debate on the use of force has already led to much debate because of its inherent complexities, with regard to the cyber domain it appears even more complex. The Tallinn Manual also takes imminence as its criterion for the right to use force in self-defence.[98] What then amounts to imminence is a complicated matter. The majority of the international group of experts that authored the Tallinn Manual rejected an approach that 'requires that the armed attack be about to be launched, thereby imposing a temporal limitation on anticipatory actions'.[99] Instead, they opted for an approach whereby 'it may act anticipatorily only during the last window of opportunity to defend itself against an armed attack that is forthcoming'.[100] This is a complicated analysis to make especially with regard to cyber operations that may take place at high speed. The Tallinn Manual therefore states: '[T]he lawfulness of any defensive response will be determined by the reasonableness of the victim-State's assessment of the situation, as well as other requirements of self-defence, in particular necessity and proportionality.'[101] However laudable this may sound, it suggests a transparency that, where a State makes an error in judgement, it would always be liable. In most cases, however, this would be highly unlikely given the character of digital traffic and the problems of attribution. And who then could make a final and authoritative determination of the reasonableness of the assessment after the fact? Given that it concerns self-defence under Article 51, that would lead us automatically to the Security Council. But it seems highly unlikely that it will be able to make such a determination since it will always involve either a P5 State, or a client State. This interpretation of imminence therefore risks crossing over into pre-emptive or preventive self-defence,[102] which rightly could be interpreted by the victim State as an armed cyber-attack; in short, it could be seen as an offensive use of force which allows for self-defence. This is an extremely dangerous and circular situation that must be prevented. The criterion of imminence in cyber defence operations therefore needs to be clarified.

Finally, some observations can be made regarding critical infrastructures in general, and in particular the production, storage and transport of dangerous goods (e.g., chemical, biological, radiological and nuclear materials) or energy installations and networks like those of nuclear power plants. Critical (information) infrastructures as discussed earlier in section 2(b) above are clear civilian objects, with civilian workers. Under the principle of distinction, which is a core principle of humanitarian law, the civilian population and civilian objects may not be the object of an attack. In the already much-quoted advisory opinion of the ICJ this was

---

97 Ibid.

98 'The right to use force in self-defence arises if a cyber armed attack occurs or is imminent. It is further subject to a requirement of immediacy': Tallinn Manual (n 85) Rule 73.

99 Ibid., 351(4).

100 Ibid.

101 Ibid., 352(8).

102 This would be contrary the position taken in the Tallinn Manual (n 85) 353, where it rejects preventive strikes: 'a preventive strike, that is, one against a prospective attacker who has not initiated any preparations or expressed either impliedly or explicitly an intention to carry out an armed attack, does not qualify as a lawful exercise of anticipatory self-defence'. See also Schmitt, 'International Law in Cyberspace (n 85) 23–4, where he remarks 'that the devil is in the detail' and then discusses positions taken by the Tallinn Manual experts on anticipatory self-defence. He, however, does not get into the question how in practice to make the distinction between a situation where anticipatory self-defence is allowed and preventive self-defence is not. (Furthermore he also discusses the non-State actor's operations.)

stressed in no uncertain terms.[103] That targeting a nuclear power plant, or a critical infrastructure concerning the production, storage or transport of dangerous goods like chemical, biological, radiological and nuclear materials, may result in similar destruction as when used as a military means does not make any difference. The rule is clear that civilian objects should not be targeted, regardless of whether it is in offence or defence.[104]

8. CONCLUSION

The questions addressed by this chapter are whether cyber deterrence comparable to nuclear deterrence is possible and, if so, whether it would be in accordance with public international law. In response, several observations can be made. Note that these observations relate to State rather than non-State actors and thus this chapter only deals with part of the problem of possible offensive cyber operations.

Deterrence in terms of Morgan[105] can be realised either via the projection of 'retaliation' or 'stout defence'. In both these cases the deterrent threat is realised by making clear that in case of a cyber-attack that amounts to an armed attack there will be a reply.

It is clear that a cyber-deterrent strategy comparable to a nuclear-strategy, with an all-out retaliatory strike in case of an (imminent) attack, at present is not possible for the reasons discussed above, such as not knowing who the opponent is or who to attribute the attack to. Deterrence by the threat of retaliation in case of an attack would, furthermore, be contrary to public international law, and some of its basic principles. Retaliation points to a possible unlimited use of force that is intended to harm a potential attacker. It amounts to a threat of force, which is forbidden under Article 2(4) UN Charter and is different from self-defence since it would be aimed at punishment and would not be based on necessity and proportionality, which are central customary law criteria for self-defence. Therefore, an effective cyber-deterrence strategy via retaliation is technically unviable. But even if it were, the projection of retaliation would amount to a forbidden threat of force. Moreover, cyber deterrence cannot be compared to nuclear deterrence for the simple reason that nuclear deterrence should be viewed as a category of its own, vested in the political reality of international relations, and apparently viewed as being 'above the law', as is clear from the ICJ's advisory opinion on the use of nuclear weapons.

Deterrence by the presentation of a convincing threat to realise both an optimal passive and active defence would be possible. Such projection of an optimal self-defence in case of a cyber-attack amounting to an armed attack is in conformity with public international law, for it makes clear that a State will make use of its right to self-defence under Article 51 UN

---

[103] *Legality of the threat or use of nuclear weapons* (n 57) para 78. See Yoram Dinstein, 'The Principle of Distinction and Cyber War in International Armed Conflicts' (2012) 17 *J of Conflict & Security L* 261, 265–6.

> The cardinal principles contained in the texts constituting the fabric of humanitarian law are the following. The first is aimed at the protection of the civilian population and civilian objects and establishes the distinction between combatants and non-combatants; States must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets.

[104] Ibid., 264.

[105] Morgan (n 49) 55.

Charter if attacked. In other words, a deterrent threat of force by a State in fact comes down to forewarning any potential attacker that it will make use of its legitimate right to self-defence, which is one of the two exceptions to the general prohibition of the use of force.

Therefore, cyber deterrence via the projection of defence is permissible. States should focus on the technical and doctrinal aspects of deterrence to project a credible defence via all possible passive and active cyber defence means at their disposal. Such a strategy would need to be transparent because, the more it convinces opponents as being a realistic strategy, the more chances it has to prevent attacks, which is the essence of deterrence. With regard to protecting critical infrastructures, this requires applying all possible passive and active defence measures and also requires constant monitoring. A transparent deterrence strategy will furthermore contribute to the defence against attacks by non-State actors. As such, it will attain its ultimate aim of deterrence.

18. Distinctive ethical challenges of cyberweapons

Neil C Rowe[1]

1. INTRODUCTION

Governments have been aggressively pursuing development of cyberweapons in recent years, most notably the United States,[2] China, and Russia. Cyberweapons are a new kind of weapon.[3] As with all weapons, ethical principles should be applied to decisions about using them. We will focus here on their use by militaries; so far there has been little threat from non-governmental groups such as terrorist organizations, though some businesses have expressed interest in using them against their foreign competition. There is much debate about how well the current international laws of warfare[4] apply to cyberweapons.[5] There is now a proposed international standard for such laws in the Tallinn Manual[6] which primarily focuses on the cyberweapons operations short of warfare; such uses have become common, while clear cyberwarfare has been rare. First however, we should identify the ethical issues involved since they guide lawmaking. Key ethical issues with cyberweapons arise in their implementation, targeting, and damage recovery. The discussion is evolving quickly since our earlier survey[7] and the Tallinn Manual has especially encouraged discussion.

To limit the size of this discussion, we will focus on those characteristics of cyberweapons that significantly differ from those than conventional weapons. Much also has been written about the ethics of conventional warfare,[8] and some of that can be applied to cyberweapons.[9] But the special characteristics of cyberweapons raise new ethical problems, especially in the

[1] This work was supported by the US National Science Foundation under grant 1318126 of the Secure and Trustworthy Cyberspace Program. The views expressed are those of the author and do not represent those of the U.S. Government.

[2] Tom Gjelten, 'First strike: US cyber warriors seize the offensive' (January/February 2013) *World Affairs Journal* 201 www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-the-offensive.

[3] Sanjay Goel, 'Cyberwarfare: connecting the dots in cyber intelligence' (2011) 54 *Communications of the ACM* 132.

[4] ICRC (International Committee of the Red Cross), 'International humanitarian law – treaties and documents' www.icrc.org/icl.nsf.

[5] Robert Belk and Matthew Noyes, 'On the use of offensive cyber capabilities: A policy analysis on offensive US cyber policy' (March 2012) http://belfercenter.ksg.harvard.edu/experts/2633/robert_belk.html. See also Arimatsu (Ch 19 of this Handbook), Bannelier (Ch 20 of this Handbook) and Gill (Ch 21 of this Handbook).

[6] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017).

[7] Neil C Rowe, 'The ethics of cyberweapons in warfare' (2010) 1 *International Journal of Technoethics* 20.

[8] Steven P Lee, *Ethics and War: An Introduction* (CUP 2012); Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (Basic Books 2006).

[9] Edward T Barrett, 'Warfare in a new domain: the ethics of military cyber-operations' (2013) 12 *Journal of Military Ethics* 4.

conduct of warfare (*jus in bello*).[10] We shall follow here a negative utilitarian approach to ethics in which we try to assess the negative cost to societies of various policies with cyberweapons and try to recommend policies that result in the least negative cost on the average. Negative utilitarianism is appropriate here because the immediate goals of cyberattacks are not especially diverse, being confined to disabling adversary computer systems, networks, and what they control.

The Stuxnet cyberattack on Iran[11] provides an example of a problematic cyberattack. Some have lauded this as an example of 'clean' cyberwarfare since it appeared to have a narrow target and achieved some tactical success against it. The target appears to have been software for industrial-control machines for Iranian centrifuges used for processing uranium, and the attacks appeared to cause destruction of some of the centrifuges. But to achieve this success, many other kinds of machines had to be infected with the malicious code ('malware') with the hope of eventually transferring their infection to the target machines. This mode of infection was like a virus, and the attack code spread to millions of machines, so the attack involved widespread tampering with software. Because the propagation methods were unreliable, redundant methods were used (apparently six), showing that its creators lacked confidence in the effectiveness of its methods. Once the attack was recognized, the new propagation and attack methods were analysed and reports were published. This enabled criminal attackers to exploit these new methods for their own purposes.[12] So there was direct collateral damage from the propagation of the attack (small damage to many machines adding up) as well as from the criminal applications of the methods.

This case suggests we should be sceptical of claims that cyberweapons are precise weapons that do not cause significant collateral damage.[13] This should be unsurprising because precision is often difficult for new weapons. Consider for instance air targeting with drones in Pakistan[14] for which 'very few' of the attacks (though it varies with the estimator) were on militants. The problem is that there are just too many possible errors in targeting when the attacker is not near the target and does not understand its context. We suspect cyberattacks will tend to be even more errant, as their targets are even more remote from the attacker and appear to be similarly low-risk to the attacker.

---

[10] Herbert S Lin, Kenneth W Dam and William A Owens (eds), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (National Academies Press 2009).

[11] Michael J Gross, 'A declaration of cyber-war', *Vanity Fair* (April 2011) www.vanityfair.com/culture/features/2011/04/stuxnet-201104. See also Bannelier (Ch 20 of this Handbook) and Gill (Ch 21 of this Handbook).

[12] Dan Kaplan, 'New malware appears carrying Stuxnet code', *SC Magazine* (18 October 2011) www.scmagazine.com/new-malware-appears-carrying-stuxnet-code/article/214707.

[13] Ryan Jenkins, 'Cyberwarfare as ideal warfare' in Fritz Allhoff, Adam Henschke and Bradley Jay Strawser (eds), *Binary Bullets: The Ethics of Cyberwarfare* (OUP 2016). See further Gill (Ch 21 of this Handbook).

[14] Stanford Law School International Human Rights and Conflict Resolution Clinic and New York University School of Law Global Justice Clinic, 'Living under Drones: Death, Injury, and Trauma to Civilians from U.S. Drone Practices in Pakistan' (September 2012) http://www.livingunderdrones.org/report/.

2. DEFINING CYBERWEAPONS

Cyberweapons are weapons that use software to target data and other software. They are usually in the form of modified versions of existing legitimate programs to control computers and devices. In a cyberweapon as opposed to cyber-espionage, these modifications are for the purpose of sabotage, to prevent a victim from using at least some parts of their computer systems or their data. A cyberweapon might prevent a missile defence system from functioning properly so that it will be destroyed by a missile. A cyberweapon might also delete key data or programs from a computer system so that it cannot do its tasks, or it could block network access so a system cannot communicate with others. Usually cyberweapons do not actively create false data, as that is more difficult to do.

Use of cyberweapons, or a 'cyber operation' in military terminology, is a special case of a cyberattack. Cyberattacks are any methods that attempt to subvert computer software or data for some gain to the perpetrator. Most cyberattacks today are by criminals and support financial fraud. They are also important to intelligence agencies as a way to steal secrets; the United States has been subjected to extensive such intelligence gathering recently. However, these are not cyberweapons, as intelligence gathering is not considered an act of warfare in the laws of war, and does not justify a counterattack in response.

Software techniques used for cyberweapons are similar to those used for criminal cyberattacks.[15] These usually involve impersonation to gain unauthorized access using flaws in the software of computers or devices, followed by installing of malicious software and covering their tracks. Criminals are becoming increasingly professional in probing well-known software for flaws and developing attack methods, and their discoveries benefit cyberweapons developers. For instance, criminals have developed ways to control machines remotely over the Internet using the techniques of 'botnets' where the attacker's machine sends orders to target machines to direct their theft of personal information or spamming.[16] Botnets have clear analogies to military command structures, so it is not surprising that the US and Chinese militaries are pursuing this approach.[17]

3. PECULIARITIES OF CYBERWEAPONS

We can identify several key differences between cyberweapons and traditional weapons:

D1. Cyberweapons do not require physical proximity of the attacker to the victim, since attacks can be accomplished over the Internet, or else set up long in advance (as 'Trojan horses') and triggered by timing mechanisms or specified events when the attacker is long gone.[18] Thus they raise ethical concerns about the ability of the attacker to remotely confirm the identity of their victim and assess continued suitability of the attack.

---

[15] Cameron H Malin, James M Aquilina and Eoghan Casey, *Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides* (Syngress 2012).

[16] Christopher Elisan, *Malware, Rootkits, and Botnets: A Beginner's Guide* (McGraw-Hill Osborne 2012).

[17] Gjelten (n 2).

[18] Randall Dipert, 'Other-than-Internet (OTI) cyberwarfare: challenges for ethics, law, and policy' (2013) 12 *J of Military Ethics* 34.

D2. Cyberweapons are easy to conceal, even easier than biological weapons since they are just abstract patterns of information. They can also operate very quickly and then destroy all evidence of their presence. This means disarmament of cyberweapons is very difficult, though some methods can help.[19]

D3. Cyberattacks can be very difficult to trace back to the attacker ('attribute'). That is because if attacks are launched across the Internet, it can be difficult to trace them in the enormous traffic of the Internet, and attackers usually take extra steps to conceal themselves; and if attacks are launched from Trojan horses already inside software, it is difficult to tell who put them there. This means that a pure cyberwar not accompanied by conventional-weapon attacks is almost impossible to justify in cyberspace according to the standards of attribution required by the law of war because no one will know who is attacking whom.

D4. Almost all cyberweapons exploit flaws in their victim's software. That is because computer systems, digital devices, and networks are carefully designed for safety and normally have many defences against sabotage. The situation is quite different from bullets and bombs which only attack the binding force of the atoms in their targets, and that is consistent for the same material no matter what the setting.

D5. Cyberweapons have considerably more variety than conventional munitions. Guns and bombs have a single purpose of violating the physical integrity of objects and rendering them inoperative by means of projectiles and explosions. Cyberweapons can sabotage operations of computer systems in many different ways, some quite subtle.

D6. Cyberweapons technology is very similar to cyberespionage technology. That is because to do both, you must gain and maintain high-level control of a victim system. Sabotage is usually just a small step more, so escalation from cyberespionage to cyberattack is tempting for aggressors. The major countries of the world are engaging in an increasing amount of cyberespionage.[20] On the other hand, the technology of conventional espionage has little in common with that of conventional military attacks.

D7. Cyberweapons tend to have more unexpected consequences than conventional weapons. That is because computer systems depend on billions of component instructions working consistently every time they are used, and just one change can disable or modify normal functioning. Similarly, when computers and devices interact over a network, failure of just one of them may cause failure of others since there is so much interdependence of systems.

D8. Cyberweapons have no legitimate uses, unlike guns and explosives. (A possible exception is 'red teaming', or deliberately attacking a system to find its flaws, but this is often too blunt a tool to be helpful.) Thus finding of cyberweapons is prima facie evidence of offensive intent.

These features have many ethical implications. In this chapter we will focus on those which we consider the most important: justifying the use of a cyberweapon, the product tampering required for cyberweapons, the unreliability of cyberweapons, collateral damage with cyberweapons, and the difficulty of recovering from the damage of cyberweapons. These relate to

---

[19] Neil Rowe and others, 'Challenges in monitoring cyberarms compliance' in Panayotis Yannakogeorgos and Adam Lowther (eds), *Conflict and Cooperation in Cyberspace: The Challenge to National Security in Cyberspace* (Taylor and Francis 2013).

[20] Adam Segal, 'The code not taken: China, the United States, and the future of espionage' (2013) 69 *Bulletin of Atomic Scientists* 38. On cyber espionage and international law see Buchan and Navarrete (Ch 11 of this Handbook).

classic ethical issues in the conduct of war of *jus ad bellum*, proportionality[21] of the attack to the provocation, discrimination[22] of combatants from noncombatants, and assigning responsibility for conduct.[23]

4. JUSTIFYING THE USE OF CYBERWEAPONS

Many of the ethical principles about starting traditional warfare (*jus ad bellum*) apply to cyberwarfare.[24] A nation must be attacked first, suffer serious harm, and have no other feasible alternatives before it can consider cyberwarfare. Traditional land, water, and air warfare involve large military entities whose existence and methods are hard to conceal and easy to trace. This is not true for cyberwarfare, following D1, D2, and D3 above. With attacks sponsored by a nation-State, the attack data used will likely have no obvious signs of origin, its implantation on victim computer systems will be stealthy and unlikely to be recorded, and its backtracing will be impossible due to obfuscation. Attribution can be proved if the attacking country's computer systems can be accessed, but that is rare. A country may have suspicions about who attacked it, but the world community needs real evidence to endorse a response following the laws of war, and there can be serious repercussions of a false accusation. Thus it is very difficult to ethically justify a counterattack in response to a cyberattack, despite the eagerness of some.[25]

However, it does make sense that a traditional military attack could justify a cyber-counterattack since attribution is much easier and cyberattacks are seen as less escalatory. Indeed, cyberattack methods might be a force multiplier for military commanders, allowing them to achieve the same results with fewer forces and with possibly less harm to both sides.[26] However, achieving less harm with cyberattacks than traditional attacks is not automatic, and each case needs to be evaluated carefully according to the criteria discussed later.

5. PRODUCT TAMPERING AND PERFIDY

A key ethical problem with cyberweapons that follows from D4, D6, and D8 is that implementing them usually must tamper with or change existing software to achieve effects.[27] This is a violation of the ethical principle of discrimination of noncombatants from combatants since nearly all software is intended for civilian use. Tampering with the tools upon which noncombatants depend hurts them. Most countries have laws against product tampering, as

---

[21] See also Gill (Ch 21 of this Handbook).

[22] See Bannelier (Ch 20 of this Handbook).

[23] Alexander Moseley, 'Just War Theory' (*Internet Encyclopedia of Philosophy*) www.iep.utm.edu/justwar.

[24] Barrett (n 9). See also Roscini (Ch 14 of this Handbook) and Focarelli (Ch 15 of this Handbook).

[25] Patrick Lin, 'Ethics of hacking back: Six arguments from armed conflict to zombies' http://ethics.calpoly.edu/hackingback.pdf.

[26] Dorothy Denning and Bradley Strawser, 'Moral cyber weapons: the duty to employ cyberattacks' in Luciano Floridi and Mariarosaria Taddeo (eds), *The Ethics of Information Warfare* (Springer 2014).

[27] Neil C Rowe, 'Cyber perfidy' in Fritz Allhoff, Nicholas G Evans and Adam Henschke (eds), *The Routledge Handbook of War and Ethics* (Routledge 2013).

it can cause widespread harm including death. In the United States for instance, the Federal Anti-Tampering Law (USC Title 18 Chapter 65, 'Malicious Mischief') defines several categories including 'whoever, with intent to cause serious injury to the business of any persons, taints any consumer product or renders materially false or misleading the labelling of, or container for, a consumer product'. This has a penalty of up three years in prison, and tampering that causes bodily harm receives up to 20 years. These laws apply to software in the category of 'device' where malicious modification renders misleading the labelling of the software. Commercial software also is generally supplied with end-user license agreements that prohibit modifications to it.

Product tampering is virtually essential to cyberweapons because computer systems and digital devices are generally very reliable and strongly resistant to attempts to subvert them for unanticipated purposes. Attacking a computer system directly by sending it malicious instructions will usually be ignored; flooding with too much data is usually controlled by rate limits on the target network. So an attacker must almost always try to change the software to perpetrate a cyberattack. Usually the target is in the operating system, the software that controls the entire computer or device. Particular targets are the security kernel of the operating system, the file-management system, the update manager, the networking software, and the electronic-mail system. These civilian artifacts are almost always implemented by civilians, and there are few alternatives to using them due to the near-monopolies by a few corporations. Making them military targets is similar to poisoning a well that a community must use.

Product tampering is perfidy if done during war. Perfidy is impersonation of civilians by military forces, and is prohibited by the laws of war to prevent higher civilian casualties. Guns, bombs, and missiles do not need impersonation to work, so cyberweapons are fundamentally different. Thus nearly all cyberweapon installation or use appears to be unethical on the perfidy criterion.

An objection the idea of cyberweapons perfidy is that cyberweapons cannot hurt people as much as other weapons. We disputed the nonlethality claim in section 1. But the Geneva Conventions do not require a death threat to civilians in its definition of perfidy; more general harm such as threats of injury and capture are also included. Just-war theory does permit 'dual-use' weapons that harm civilians as well as military targets when the military benefit is high, but attacking almost-exclusively civilian targets cannot support dual use. That is what most cyberweapons do.

It has been argued[28] that cyberweapons should be ethically superior to traditional weapons because of their relative nonlethality,[29] and thus their perfidy could be excused if warfare is ethically justified. Yes, if you could be sure of getting the effect of a kinetic attack by a cyberweapon, it could be preferable to a conventional weapon. However, the unreliability of cyberweapons discussed in the next section means that a cyberweapon is less likely to be effective and that trades off with its nonlethality. Cyberweapons also tend to cause plenty of collateral damage as we discuss later. Human life has a finite value, usually assessed by economists as a few million dollars, and cyberattacks can cause millions of dollars in collateral damage. So the monetary damage of nonlethal cyberweapon may be worse than a weapon that kills.

---

[28] Denning and Strawser (n 26).
[29] Jenkins (n 13).

6. THE UNRELIABILITY OF CYBERWEAPONS

Another key problem with cyberweapons that follows from D1, D4, and D7 is that they must exploit flaws in human artifacts, generally flaws in software. Flaws may get fixed unexpectedly since software experts are always trying to find them and fix them. That means that some targets without flaws are unattackable regardless of their strategic importance, and success against other targets may be uncertain and depend on the chance that the flaw has been found, the chance that a fix for the flaw has been found, the chance that the fix has been disseminated, and the chance that the target has installed the fix. Control of the cyberweapon may also be unreliable, since it may depend on Internet connections that are untested until conflict or are likely to be deliberately broken once a conflict begins. This means that cyberweapons will be quite unreliable. They can be more reliable if the victim standardizes their software and hardware too much, as the US military tends to do, but there can still be surprises when systems are used in untested ways. In addition, routine maintenance on software can install new versions, reorganization of a network can give new configurations, or the target may engage in deliberate deception, all of which can make a cyberweapon useless.

Unreliability means there is a risk of violating both the ethical principles of discrimination of noncombatants[30] and proportionality[31] of attacks to the provocation. Discrimination is at risk because it is difficult to see what you are attacking in cyberspace and what effects your attacks have, and particularly with military organizations who keep their digital assets well protected from probing. Plenty of errors occur even with conventional weapons. Errors occur with air targeting when intelligence is outdated, as with the US bombing of the Chinese embassy in Belgrade in 1999, or when people or buildings are misidentified, as with bombing of a Red Cross warehouse in Afghanistan in 2001.[32] Cyberspace provides additional opportunities for mistakes in targeting because the range of operations is large, camouflage is easy, and large changes to the target can be made quickly. The Red Cross warehouse was bombed even though it had a large red cross on its roof because the bombing pilots flew too high to see it. There will likely be even more problems with identifying the context of a target in cyberspace and metaphorically seeing a 'red cross'.

The unreliability of cyberweapons also encourages commanders to use disproportionate massive and multifaceted cyberattacks to ensure a desired effect. For instance, Stuxnet used at least six propagation methods when only one was necessary. No commander wants to use insufficient force against a target. However, overkill results in unnecessary damage if the attacker underestimates the chances of success, and unnecessary damage is unethical and prohibited by the laws of war. Underestimation will be frequent with cyberweapons because the conditional probabilities of one attack method succeeding when another succeeds are not independent but positively correlated in unpredictable ways, since there can be hidden common underlying vulnerabilities that both methods can exploit. Thus overkill can easily happen with cyberweapons.

The US in particular favours overkill with conventional weapons, as in Iraq in 2003 when commanders freely admitted they wanted to create 'shock and awe' (alias terror). So it is likely that the US will favour overkill with cyberweapons, hoping that the victim country

---

30 See Bannelier (Ch 20 of this Handbook).
31 See Gill (Ch 21 of this Handbook).
32 Alex J Bellamy, *Just Wars: From Cicero to Iraq* (Polity 2006).

cannot respond with counter-cyberattacks on a similar scale. But the US military does not have the military superiority it once did due to major adversaries. Nonetheless, software vendors continue to sell the US military all kinds of capabilities. Cyberweapons are a very appealing product for vendors to sell since they are software that is rarely used, can be made to look good in artificial test conditions, and will likely fail in real conflict only long after the vendor has been paid.

Another reliability problem is that automated or semi-automated cyberweapons may not be stoppable after terminating hostilities, a violation of the laws of war on armistices (which derive from the ethical principle of responsibility for warfare). Cyberweapons not controlled from the Internet, as those set to work at a predetermined time, would risk this. But even with Internet-controlled cyberattacks, once a victim recognizes they are under attack, they would likely close suspicious network ports and terminate suspicious running processes, which could break the Internet connection being used to control the attack and prevent it from being stopped. This suggests that an ethical cyberattacker must either carefully design attacks to be short and risk being ineffective, or else use difficult mechanisms of control that are resistant to victim interference but are unreliable themselves. Timing channels, which convey hidden information in the times of events, are an example of a possible but difficult method of control.

Unreliability also has strategic implications. There is not much deterrence value in advertising the possession of a cache of cyberweapons, since many of them will not work, and advertising enables potential victims to better defend themselves since they can start hardening their defences and filtering out traffic from the threatening country. The main reason for a State to assemble military assets is in their deterrent effect, and cyberweapons will not provide this. The lack of a deterrent effect also encourages surprise attacks since they can be more effective than attacks for which advance warning has been provided. Surprise attacks usually are unethical and violate the laws of war since responsible countries should strive to defuse conflict situations before attacking. Another strategic issue is that unreliable weapons are poor choices in a conflict since there are many reliable weapons that better ensure proportionate and discriminatory responses. It thus could be unethical for a commander to use a cyberweapon when other weapons are available.

7. COLLATERAL DAMAGE

Perhaps the most serious ethical problem with cyberweapons is their potential for collateral damage to civilians due to D1, D5, D6, and D7. This can violate the ethical principle of discrimination of noncombatants.[33] Cyberattack methods have been employed so often by criminals against civilians that it is doubtful that cyberweapons will be applied only to military targets. The definition of a civilian is increasingly unclear in modern warfare,[34] and increasing

[33] Jack McDonald, 'Blind justice? The role of distinction in electronic attacks' in Mariarosaria Taddeo and Ludovica Glorioso (eds), *Ethics and Policies for Cyber Operations* (Springer 2017).

[34] Pauline Kaurin, 'When less is more: expanding the combatant/noncombatant distinction' in Harry Van Der Linden, John W Lango and Michael W Brough (eds), *Rethinking The Just War Tradition* (SUNY Press 2007). See also Bannelier (Ch 20 of this Handbook).

rates of collateral damage in modern warfare are apparent.[35] The US has claimed for many of its drone strikes in Pakistan that any military-age males killed must be combatants, so we will undoubtedly hear a similar argument from any aggressor about the victims of their cyberattacks during cyberwarfare. But we can generally identify civilians as people with not contributing substantially to warfare by their activities or products, or most of the world.

(a) Lethality of Cyberattacks

Some have argued that cyberweapons are 'nonlethal' and potentially ethically desirable compared to other weapons.[36] Mortality is not the only harm in warfare, as we will discuss further. However, allegedly 'nonlethal' weapons can still kill people, as for instance as crowd-control foam from which people can suffocate, since nearly any method of human control can be lethal in unexpected circumstances. Cyberweapons can kill directly as when they interfere with operations at hospitals or in industry (Iran alleges that Stuxnet caused an explosion of a centrifuge that killed a worker). Cyberweapons can also kill indirectly by damaging the infrastructure of a society. For instance, it has been estimated that the damage to Iraqi society by the conventional weapons of the US invasion in 2003 resulted in a 654,000 additional deaths 2003–2006 of which 92 per cent were due to violence,[37] plus another estimated 300,000 deaths through 2011 due to damage to the Iraqi infrastructure.[38] We need to evaluate lethality of cyberweapons with the same standards as those of other weapons.

(b) Types of Collateral Damage from Cyberattacks

Harm need not be measured in human deaths; discussions in the field of ethics have increasingly addressed harm to other living things,[39] and some have proposed that harm to digital systems is morally wrong regardless of whether humans are harmed.[40] So we need to consider a broader definition of harm.

Cyberattacks involve manipulation of programs and data and there are many ways to do this. Ideally, a cyberattack should modify something critical to warfighting; we call these type-0 cyberattacks. They are consistent with the standard goal of warfare to interfere with a victim's ability to wage war, which is a more ethical goal according to the notion of proportionality than just causing damage to provide a deterrent effect. Consider the software for

---

[35] Thomas W Smith, 'The new law of war: Legitimizing hi-tech and infrastructural violence' (2002) 46 *Intl Studies Quarterly* 355.

[36] Jenkins (n 13); Denning and Strawser (n 26).

[37] Gilbert Burnham and others, 'Mortality after the 2003 invasion of Iraq: a cross-sectional cluster sample' (2006) 368 (9545) *The Lancet* 1421.

[38] Amy Hagopian and others, 'Mortality in Iraq associated with the 2003-2011 war and occupation: findings from a national cluster sample survey by the University Collaborative Iraq Mortality Study' (2013) 10 *PLoS Medicine*, https://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1001533.

[39] Peter Singer, *Animal Liberation: The Definitive Classic of the Animal Movement* (Updated Edition Harper Perennial 2009).

[40] Patrick Smith, 'Towards a richer account of cyberharm: the value of self-determination in the context of cyberwarfare' in Daniel Ventre (ed), *Information Warfare* (Wiley 2016).

a missile-defence system, as in the Israeli quasi-cyberattack on Syria in 2007;[41] a cyberattack could replace software for missile defence on a victim's system with a copy that will malfunction in critical situations. Unfortunately, these type-0 cyberattacks are very difficult to do, as software critical to an ability to wage war is highly protected. Any potential victim should be running integrity checks periodically on their critical software to make sure it has not changed; recalculating hash values on the software is the standard way. So type-0 cyberattacks are usually infeasible. They are also unlikely to accidentally hurt civilians because warfare-related software has few civilian uses.

A cyberattack could modify data on which target software depends; if these changes reach civilians, we can call this type-1 collateral damage. An example would be modifications to a 'configuration file' that defines the operating parameters for some software. But most modifications of configuration files will not disable software since that would be poor software design, and those that do should reveal their presence by causing failure in more than the targeted conditions.

A cyberattack could target general-purpose software on which a military organization depends such as networking software. Such software is not as well protected as military-specific software since usability is often more important than security for the vendor. Since such software is usually downloaded from repositories, it would be more effective for a cyberattack to modify the downloadable copy to create a 'Trojan horse' whose malicious intent is concealed. If civilians also download it, we call this type-2 collateral damage. If the downloading itself is concealed from the victim, as when files from a USB thumb drive are automatically downloaded to a computer in which they are inserted, we call this type-3 collateral damage; it appears to have been a key method in propagating the Stuxnet attack.[42] Collateral damage of type-3 attacks can be worse than type-2 attacks because tracing the source of the malware is harder, making diagnosis and repair more difficult.

Finally, attacks can spread to a victim from viruses and worms that commandeer parts of legitimate programs to enable their spreading. If they spread to civilian systems, we call that type-4 collateral damage. Collateral damage is a serious risk with these methods because it is hard for software to recognize civilian software and data, as discussed in more detail in the next section. Viruses and worms also need to be kept as small as possible to aid in their concealment, so there is often insufficient room for code to carefully examine what they are attacking. In addition, security software looks constantly for them, so they have a high failure rate. That means that Type-4 attacks are too blunt and ineffective to be appropriate for most cyberwarfare, and are thus unethical.

(c) Discriminating Military from Civilian Targets

Stuxnet did well at discriminating centrifuge systems from civilian systems for purposes of sabotage, as it looked for certain specialized process-control software. Stuxnet was poor, however, at discriminating civilian systems for purposes of propagation of the attack code, and propagated onto millions of civilian systems. It is desirable that a cyberweapon check the

---

[41] Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (HarperCollins 2010).

[42] United States Cyber Consequences Unit, 'Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008: US-CCU Special Report' (August 2009) http://www.usccu.us/.

address of the site it is on, the kind of software the site is running, the kinds of network protocols it is running, the kind of files on the systems, the kinds of encoding used for transmissions, and so on, to be even more sure what system it is on before doing damage.[43] Unfortunately, this is impossible for some popular types of cyberattacks that are inherently broad. The denial-of-service cyberattacks on Georgia in 2008 were predominantly against civilians[44] even though they supported a military operation. That is because denial of service is a rather indiscriminate weapon; it slows down not just targets but any other sites on shared networks, and military organizations often share network resources with civilians.

Identifying military sites from their Internet addresses or site names is also very difficult. Directories of military Internet sites provide only broad detail so they do not discriminate a military command from a military hospital or military housing, as more specific information would enable better cyber-targeting. A potential target may also distribute false address information, deliberately create decoys to encourage attacks on the wrong targets, or camouflage valid targets with false names, as those are standard military tactics. Or a criminal may spoof a military site to gain leverage or cause mischief.

As for using the internal data on a system to decide if it is a military target, the information that a cyberweapon can extract about its environment will be mostly unhelpful technical data. There is no standard for labelling systems internally to indicate their purpose. Explicitly labelling military sites would increase the danger to them. Examining the files on a system is also a poor way of deciding whether it is military. Military organizations use mostly civilian software because it is cheaper than the alternatives. The few software products used only by military organizations could be clues to the identity of a system, but extensive intelligence is necessary to identify what they are and what files they are associated with. The names that sound the most military on systems are often games. So determining that a site is military requires thorough espionage, but thorough espionage is more likely to be discovered, and makes it less likely that a subsequent attack will be effective.

A key ethical dilemma of warfare in the last 100 years has been the increasing fraction of casualties that are civilian. Electrical grids are increasingly military targets;[45] for instance, much collateral damage to civilians in Iraq in 2003–2004 occurred due loss of electrical power when utilities such as communications, water systems, and refrigeration stopped. Civilians depend more on the electrical grid than militaries do since militaries have better backups like generators and batteries. This, however, does not mean we must accept high civilian casualties with cyberweapons since the ethical obligation to minimize suffering of innocent people has not changed. In fact, we should be able to control cyberweapons better than other kinds of weapons because of their digital nature.

---

[43] David Raymond and others, 'A control measure framework to limit collateral damage and propagation of cyber weapons' in Karlis Podins, Jan Stinissen and Markus Maybaum (eds), *2013 5th International Conference on Cyber Conflict* (CCD COE Publications 2013).

[44] United States Cyber Consequences Unit (n 42).

[45] Smith (n 35).

8. REPAIRING THE DAMAGE OF CYBERATTACKS

Another major ethical problem with cyberweapons is repairing their damage after the end of hostilities (*jus post bellum*), something that can be quite difficult due to D2, D3, D5, and D7. This risks the ethical principle of proportionality[46] of attacks in a different way. Unless the effect is obvious, it can be hard to locate the damage due to a cyberweapon since it may not be visible excepted to highly specialized tools. Software and systems are interconnected, and what may appear to be a flaw in one may actually be a flaw in another. Thus using some kinds of cyberweapons may be sentencing the victim to years of damage repair. This is particularly true for less-developed victim countries without much technical infrastructure. So indiscriminate cyberweapons could be even worse to clean up afterwards than the land mines or improvised explosive devices which completely reveal themselves with the attack.

Finding the damage of a cyberattack when clues are poor can be technically difficult. Software tools can keep hash values on files as a quick way to determine if a file has been changed, but such tools are only rarely used. However, files change routinely with updates and modifications of their data, and there is no easy way to tell whether a file has been changed legitimately or maliciously. Also, cyberattack code and data can hide outside the files of a system in the storage not being used by the operating system ('slack space') or in fragments of deleted files left in storage after they have been marked for permanent deletion.[47] Neither of these two places can be accessed by the operating system so they cannot be searched. In addition, files merely marked for deletion can be impossible to access as well on most mobile phones without destroying the phone. So there are many opportunities for cyberattack code or data to hide well.

(a) Repair Methods

The usual approach to damage repair from criminal cyberattacks is to try to restore the damaged systems from backup data. This can be done for cyberwar cyberattacks too, but it is more difficult. Backup restoration will not work if the attack code remains in the hardware, firmware, or in the boot code (such as BIOS). Restoring can take a long time since usually an entire operating system should be restored to remove all possible sources of reinfection. Cyberattacks can hide in data as well, and the data may need to be restored from backup too. Not all systems make adequate backups, since it is a tedious and rarely useful task, and they may be incomplete, faulty, or even entirely missing, and then most of the damage of a cyberweapon could be permanent. In addition, cyberattacks can also cause damage in the form of opportunities missed while the system was under attack.

Another problem is that new damage from a cyberweapon may persist a long time if it used automatic propagation. The Stuxnet attacks continue to circulate today; though their volume has been reduced by antivirus software, not everyone has antivirus software nor has it configured correctly. So even if a system is restored from backup, it may be reinfected if not all propagation methods have been discovered and countermeasures applied. Since cyberweapons will tend to use novel methods of attack, this can be a challenge.

---

[46] See Gill (Ch 21 of this Handbook).

[47] Richard Boddington, *Practical Digital Forensics* (Packt Publishing 2016).

For these reasons an ethical cyberattacker should take steps to facilitate damage repair after the cessation of hostilities. First, an ethical cyberattacker should publicly acknowledge and describe their attack after hostilities because the attacker knows what they attacked and how, and can provide the best guidance as to what to repair. This is a form of the ethical principle of responsibility for conduct in warfare. Acknowledgement can be announced, but it is better to prove it by attaching cryptographic signatures to the attack, so false claims of responsibility can be prevented. In fact, it may be desirable for a country to take responsibility for an attack at the time of the attack to obtain political leverage. The close connection of cyberespionage to cyberwarfare makes this difficult for intelligence agencies to accept, since espionage tries to avoid attribution, but warfare is fundamentally different from espionage and subject to many more international agreements.[48] Second, at the cessation of hostilities an ethical cyberattacker should provide sufficient information to the victim to enable them to quickly locate all the damage, perhaps in the form of lists of sites and software on those sites. This would be similar to keeping records of where land mines have been emplaced. Third, an ethical cyberattacker should use attack methods that are easy to repair. That means avoiding autonomous propagation methods as much as possible, and preferring actions that are easily reversible.[49] An example of the latter is encryption of key data by the attacker; then the attacker can decrypt the data at the cessation of hostilities and exactly restore what was there before, since encryption preserves information.

(b) Costs of Direct Damage from a Cyberweapon

We would like to quantify the collateral damage from cyberweapons. Recovering from a cyberattack requires removal of malware-infected files and malicious processes, and the cost can vary considerably with these targets. It may also require removal of vulnerabilities in otherwise blameless software that led to the cyberattack ('patching'). Sites such as cert.org provide guidance on how to do such patches for specific types of attacks with specific indicators. But these are unlikely to be useful against cyberweapons as the attacks are likely to be novel and resistant to known patch methods. A victim that follows a patching strategy will have many difficulties, and it may cost anywhere from $1,000 US to $10,000 US.

The safest approach for the victim in most cases is to restore the entire operating system. Restoring an entire operating system requires some time, though not all human-supervised. If there are backups, some tedious labour will be needed to find and copy them. Restoration of operating systems destroys the data on the systems, which will cost additional effort to restore if it was backed up. The people doing this work need a certain level of technical knowledge, so the overall cost should be several $1,000 US per system. However, if there are no backups for some or all of the software or data, the cost of permanent data loss can be considerably more. A lack of backups, in fact, could be a good reason to target a system with cyberweapons.

(c) Costs of Attack Propagation

Cyberspace is highly interconnected, and attacks that are designed to propagate themselves can spread from a military system to civilian systems, a kind of damage analogous to the prop-

---

[48] See Buchan and Navarrete (Ch 11 of this Handbook).
[49] Rowe (n 19).

agation of biological weapons;[50] biological weapons are now banned by several international treaties. Military Internet sites are not easy to access, so attacks like Stuxnet need to propagate onto civilian machines to have a chance of reaching those targets. Even when the propagation does not damage the target system, it can hurt it by burdening the operating system with added processes and files. Those additions may be flagged by anomaly-based malware detection mechanisms, and may require time-consuming administrator inspection well out of proportion to their size. An ethical cyberattacker should design the attacks to remove themselves from stepping-stone sites after their goals have been accomplished, much in the way that the police should not linger on private property while pursuing a criminal crossing the property, but Stuxnet did not successfully eliminate itself. Propagation of damage to civilian systems is made easier by the fact that militaries use much of the same software as civilians such as operating systems, Web browsers, document processors, and networking protocols.. Thus it is not difficult for an attack disabling a military site to disable a civilian site that it reaches by mistake using the same mechanism.

If we assume that the average network node has K connections, and if we assume that the chance of propagating the attack to a new node is p, then we should expect from a single attack p*K infections from immediate neighbours, and $p^M K^M$ infections in neighbours M steps away. If pK<1, the number of total infections can be calculated by a geometric series whose sum is $1 / (1 - pK)$, so we can multiply this by the cost of repair of a single system to get the overall cost of an attack. But if pK>1 the propagation is unbounded through a population of vulnerable systems, and that was apparently true of Stuxnet. Stuxnet was only stopped when it ran out of vulnerable machines it could reach. Usually if an attack is detected on one computer of a local-area network, the rest of the network usually receives patches, repair, or restoration as well to ensure it is safe. This multiplies the cost of an individual system repair by the size of the network, which considerably increases costs.

Countermeasures are eventually found for attacks, and the propagation rate should decrease over time. However, many computer systems and devices never get any countermeasures, due to lack of funds, carelessness, or previous cyberattack. Thus there often remain a residual set of machines willing and able to spread an old cyberattack. This means that propagation of attacks can continue a long time, incurring additional costs.

(d) Costs of Attack Analysis and Mitigation

The damage cost of a cyberattack also should include the cost to analyse it, since failure to analyse means it can continue to cause damage to new machines. This is particularly important for cyberweapons since they need to be novel to be maximally effective. Analysis includes finding methods to recognize the attack, repair its damage, strengthen defences against it, extract signatures of the attack for use by anti-malware software, and publish the findings.[51] During cyberwar, it can also be politically important to identify the country that is responsible for the attack ('attribute' it). Attribution can be costly because routing information is generally short-lived and cyberattackers deliberately make it still more difficult by using encryption, proxy servers, spoofing (impersonation), and long chains of control.

---

[50] Rowe (n 7).

[51] 'Flaw finders go their own way', *TechRepublic* (26 January 2005) http://www.techrepublic.com/article/flaw-finders-go-their-own-way/.

Cyberweapons will likely incur higher costs for analysis than criminal cyberattacks because they have the resources of nation-States for their development. Thus besides being more novel, they will be better tested, more likely to be obfuscated to make analysis difficult, and require more work to find countermeasures. Hence even if cyberattacks on military targets do not propagate much to civilian systems, they may incur significant cost to civilians because of the resources that must be diverted to analyse and protect against them.

Will some military victims try to conceal attacks to maintain military secrecy, thereby depriving the world community of useful intelligence about the attack methods? It would not be ethical, given that most attacks on military systems also work against civilian systems. It is unlikely because most victims will be weaker than their attackers (otherwise they would not be attacked) and often want all the international help they can get. Even if a victim does not reveal an attack, it may still be detected by third parties by its collateral damage, as with the discovery of Stuxnet by the Russian Kaspersky company.

Analysis, repair, and fixing for cyberattacks can be costly because it needs highly trained professionals. Much of this work is done by civilian infrastructure today since civilians bear the brunt of cyberattacks. Initial clues are provided by observations of odd behaviour reported on bulletin boards and blogs such as Bugtraq (at www.securityfocus.com) and those of software vendors for their user communities. Discussion on those sites tries to narrow down the circumstances of the behaviour and attribute it to particular features of the software. Professionals at Mitre study these discussions and decide whether it represents new vulnerability (which is usually due to a software bug); if so, they give it a CVE number at www.cve.mitre.org which represents the vulnerability's de facto label in subsequent discussions. Security professionals then plan remediation; usually the responsibility is that of the software vendor, but in the case of serious problems, independent consultants or governments may also be involved. Remediation usually requires testing by the vendor to find a complete set of fixes. The fixes usually involve changing the original vulnerable software or its configuration parameters. If the vulnerability is serious enough, it described, including signatures for identifying it and proposed remediation measures, at sites such as www.kb.cert.org (the US-CERT Vulnerability Notes Database) and www.web.nvd.nist.org, which represent de facto official recognition. Attribution of software requires further high costs.

Damage can be caused by countermeasures themselves. Worldwide damage to DNS services due to China's efforts to prevent its citizens from going to certain websites has been identified.[52] Such collateral damage can occur after attacks when victim States attempt to block network services that led to the attack. In addition, posting information about the vulnerability or attack is essential to enabling people to defend against it, and the more openness of the information exchange, the more quickly that thorough remediation measures will be found. But this openness has a price: It facilitates new attacks using the same methods. Once criminals know where the vulnerability is and roughly what it involves, it greatly simplifies their search for how to exploit it. The consensus of the information-security community today is that openness is more important than preventing new attacks in the short term, and only a few vendors disagree with that. But not all systems are fixed quickly, and cyberattackers have a window of opportunity ranging from a few days to a few weeks for systems that are lagging

[52] Sparks and others, 'The collateral damage of Internet censorship by DNS injection' (2012) 42 *ACM SIGCOMM Computer Communications Rev* 22.

in updates. Millions of dollars' worth of damage can occur in this time period due indirectly to the reporting of the potential or actual attack.

Therefore, 1,000 hours of the time of trained personnel would be a reasonable guess for the analysis, repair, and countermeasures for a cyberwarfare attack, for a total cost of US $100,000. Stuxnet was sufficiently novel that considerably more effort was expended in its analysis, so $1,000,000 is a better figure for it. Ethically, the perpetrators should be paying this cost to the non-Iranian professionals around the world for these attacks, since no state of war existed between Iran and other countries at the time. This sort of widespread collateral damage has no counterpart with bombs and missiles.

(e) Psychological Damage

Cyberweapons encourage mistrust of a victim in their military systems since attack machinery can be well hidden. When a victim is attacked or discovers a weapon, they are likely to feel insecure and suspect that other attacks are coming or other weapons are concealed. This means that some of the damage of a cyberweapon is psychological, and this can deter a counterattack.[53] This damage can extend well beyond military systems because an effective cyberattack will likely be publicized by the victim to gain international sympathy, and this will reduce the confidence of civilians in their digital infrastructure in general. While this provides a multiplier on the military effectiveness of a weapon, it creates a degree of collateral damage that is difficult to predict. Militaries prefer predictable weapons.

Psychological collateral damage is difficult to measure because it may relate little to the actual damage. Major damage to a country's military can have dramatic political consequences, as in Argentina after the Falklands War, or civilians may just interpret the damage as the military's own problem with little impact on themselves. The Stuxnet attacks led Iran to retaliate by attacking US targets to very little effect,[54] wasting resources that could have better spent elsewhere in Iran. The terrorist attacks on the US in September 2001 induced an overreaction that has not found any significant subsequent threats despite intensive intelligence collection.[55] Cyberweapons, with their mysterious modes of operation and concealed effects, are even better at inducing overreaction and fear in a population. Therefore, cyberweapons that cause broad psychological damage, such as unnecessarily powerful cyberweapons that shut down cyberspace for weeks, could be unethical regardless of their targets.

(f) Summing up the Costs of Collateral Damage

Many of the abovementioned costs of collateral damage can be measured, so we can apply utilitarian ethics. Take Stuxnet as an example. We conservatively estimate that 10,000,000 machines were infected worldwide by the attack code using multiple propagation mechanisms. Although these infections did not sabotage most of these machines, that was not obvious at

---

[53] Martin C Libicki, 'Cyberwar as a confidence game' (2011) 5 *Strategic Studies Quarterly* 132.

[54] Siobhan Gorman and Danny Yadron, 'Banks seek U.S. help on Iran cyberattacks', *Wall Street Journal* (16 January 2013) http://online.wsj.com/news/articles/SB10001424127887324734904578244302923178548.

[55] Paul R Kimmel and Chris E Stout (eds), *Collateral Damage: The Psychological Consequences of America's War on Terrorism* (Praeger 2006).

first, so quick detection and removal on each machine was important. The cost of discovery and mitigation was at least $1,000,000 as discussed above. The automated detection and removal of the Stuxnet code from the infected machines was bundled with handling other threats by anti-malware software, and so its amortized time cost was probably around a second of a user's time, hence their cost was around 10,000,000 * $100 per hour / 3600 seconds = $277,000. Attempts at determining the source of the attack probably cost around $500,000 since it had political implications. The reuse of the attack methods by criminals probably resulted in 10,000 attacks worldwide of varying costs and successes but probably averaging at least $100 per incident, for $1,000,000 total. The psychological cost to Iran was at least $500,000 just from the cost of the wasted attacks on the US. Thus the total collateral damage of Stuxnet was at least $3.4 million. There was a benefit to the attacker, a delay of a few months in Iran's nuclear development, but Iran is continuing to develop nuclear weapons and the attack does not seem to have changed that, though diplomacy may have.

Thus the damage of a cyberattack that does not kill anyone could easily reach into the millions of US dollars. One much-cited study[56] assigns a value to a US human life at $4.7 million based on economic impact, and the US government has assigned values ranging from $6 million to $9 million recently.[57] Since this value has a large economic component, it will be less in countries where per capita income is less. The international standard for insurance purposes is $50,000 per future year of human life,[58] which would give a value of $2 million for an average adult. Thus the damage of Stuxnet was similar to that of killing a person even if we do not believe Iranian claims that it killed someone. Thus the harm of a less well planned cyberattack could be greater than the cost of traditional military operations to achieve the same goals.

9. CONCLUSIONS

Cyberweapons are yet another step in the institutionalization of cowardice. With them the attacker is even more remote from their victim than with extrajudicial executions by US drones in the Middle East today. This means further opportunities for errors and misjudgements in targeting, and further opportunities for collateral and persistent damage. This is consistent with the observations and arguments that modern high-technology warfare will and must increasingly target civilians.[59] Worse, much of the damage will be hidden or disseminated across networks, so aggressors will not get adequate feedback about what they have done, and victims may find it difficult to remove the damage after the end of hostilities. Cyberweapons also embody some serious ethical problems on their own beyond collateral damage, since they are so close to cyberespionage in methods that it is very tempting to use them for small provocations,. They also usually demand cyber perfidy, and their dependence on software flaws

---

[56] W Kip Viscusi, 'The value of life: estimates of risk by occupation and industry' (2004) 42 *Economic Inquiry* 29.

[57] Binyamin Appelbaum, 'As U.S. agencies put more value on a life, businesses fret', *The New York Times* (16 February 2011) https://www.nytimes.com/2011/02/17/business/economy/17regulation.html.

[58] Kathleen Kingbury, 'The value of a human life: $129,000', *Time* (20 May 2008) http://content.time.com/time/health/article/0,8599,1808049,00.html.

[59] Smith (n 35).

makes them unreliable and inviting of overkill. Thus cyberweapons are poor options when one is trying to wage ethical warfare.

Thus a civilized country needs to think carefully before using cyberweapons. It is becoming increasingly important to resolve cyberconflicts without the violence of cyberattacks, as reducing violence is a desirable goal in cyberspace just as for other forms of warfare.[60] Because of this host of ethical challenges associated with cyberweapons, their use should be discouraged, and international agreements should be sought to restrict their use and strive for disarmament, much in the manner of nuclear, chemical, and biological weapons.

[60] Daniel J Christie and others, 'Peace psychology for a peaceful world' (2008) 63 *American Psychologist* 540.

19. Classifying cyber warfare

Louise Arimatsu[1]

1. INTRODUCTION

Human interaction in all its aspects has been radically transformed by the advent of digital technologies that now form an integral part of daily life. The extent to which this technology has unsettled long-held assumptions is only beginning to be understood, as are the legal implications thereof. For instance, it has disrupted orthodox conceptions around time and space; collapsed traditional divides between the public and private, civilian and military, domestic and international; and has redistributed and even redefined power thereby calling into question the role of the State and the interests it is expected to protect in furtherance of peace and security. Each of these disruptions – conceptual and material – and the fact that digital technologies are transforming the nature of inter-State relations as well as the relations between the State and individuals has wide-ranging implications for international law.

There is broad consensus among States that international law, including the UN Charter, and international human rights law apply to the digital realm as does international humanitarian law, despite some political resistance.[2] Further agreement has been difficult to reach and paradoxically attempts by States to cast some light on how specific rules and principles apply have led to disagreement and worse, to expose fundamentally different conceptions around some core norms of international law, even among allies.[3] Although not insoluble, the challenge of applying and interpreting international legal norms and principles in the cyber domain are potentially immense whether in the context of 'peace' or war.

[1] The author would like to thank the Arts & Humanities Research Council (Feminist International Law of Peace and Security project) and European Research Council (Gendered Peace project) for enabling her to find the time to work on this chapter. All websites last accessed on 20 March 2020.

[2] United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Communications in the Context of International Security, A/68/98 (24 June 2013) para 19 and A/70/174 (22 July 2015) section VI. On the applicability of international human rights law, see Human Rights Council resolutions A/HRC/20/8 (5 July 2012) and A/HRC/26/13 (14 July 2014) and General Assembly resolutions 68/167 (18 December 2013) and 69/166 (10 February 2015). On the applicability of international humanitarian law, E.U. Council Conclusions, General Affairs Council meeting, 25 June 2013, 11357/13; NATO, Wales Summit Declaration, 5 September 2014, para 72; Commonwealth Cyber Declaration, 20 April 2018, 4, para 4. See also Report of the Secretary-General, 9 September 2013, UN doc. A/68/156/Add.1, 15 (II. Replies received from Governments; Japan).

[3] This is best exemplified by the differences that have emerged over whether a cyber operation can constitute a breach of sovereignty *per se* (in short, is sovereignty a principle or rule in its own right?). For the UK position, see https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century. For an alternative view, see France and Netherlands at https://ccdcoe.org/library/strategy-and-governance/?category=intl-law-statements and the US at https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf.

In existing armed conflicts States are increasingly trialling their cyber capabilities alongside traditional kinetic operations.[4] That international humanitarian law applies to cyber operations conducted in the context of an existing armed conflict is a view shared by most States, the International Committee of the Red Cross and legal experts.[5] The taxing legal challenges have been to resolve how *specific* international humanitarian law rules apply, whether additional rules are needed and whether a cyber operation alone can trigger an armed conflict in the absence of an existing conflict. This latter question is becoming far more pertinent given the increasing militarization of the cyber domain exemplified by the trend among the most technologically advanced States to extend to their armed forces expansive strategic and operational decision-making powers.[6] The frequency and intrusiveness of hostile cyber operations among and between these States has increased significantly since 2012.[7] The shift from defensive to offensive cyber operations coupled with the fact that on a technical level, distinguishing between 'access' and 'effects' operations are often difficult to assess, is fuelling a culture of growing mistrust. In the cyber domain State power is being demonstrated not through threats but through conduct.[8] Against this backdrop the serious consequences caused by some operations that have been directed at civilian infrastructure (including in ongoing conflicts) which have had adverse ripple effects globally makes the need for meaningful diplomacy, genuine dialogue and a common understanding among States as to what conduct is *prohibited* by international law, and why it is so, that much more pressing.[9]

---

[4] Cyber operations are commonly used in conjunction with kinetic operations for intelligence gathering, disinformation and propaganda although in some cases operations have been directed at critical infrastructure as in the case of Ukraine; https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/.

[5] See footnote 2. Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) rule 80 [hereinafter Tallinn Manual]; and ICRC Position Paper, *International Humanitarian Law and Cyber Operations during Armed Conflicts* (28 November 2019) [hereinafter ICRC position paper] https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts. For comment on differences between States, see Michael N Schmitt and Liis Vihul, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms' (30 June 2017) *Just Security*, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

[6] For example, National Security Presidential Memorandum 13 of 2018 – which remains classified – allows USCYBERCOM to engage in cyber operations that fall below the 'use of force' and to do so without executive approval marking a departure from the policy in place under the Obama Administration; https://fas.org/irp/offdocs/nspm/index.html. See also CYBERCOM's 'persistent engagement' strategy, which came into force in early 2018 with the release of the 2018 Department of Defense Cyber Strategy and US Cyber Command's 2018 Command Vision. This strategy involves continually confronting the adversary in the cyber domain and defending against attacks as close as possible to their origin including within the adversary's networks. This new strategy is justified on the basis that mutual understanding is better reached through operational interaction rather than through policy or indeed law; https://www.defense.gov/explore/story/Article/1896846/cyber-flag-exercise-focuses-on-partnerships/.

[7] See https://www.cfr.org/interactive/cyber-operations#Timeline and sabotage/data destruction for some of the most serious cyber operations since 2005.

[8] 'An Interview with Paul M. Nakasone' (2019) 92 *Joint Forces Quarterly* 4.

[9] Notwithstanding common agreement that a State 'should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public'; Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174 (22 July 2015) 13(f). States continue to target

Lack of legal clarity and the escalation of offensive cyber operations outside 'armed conflict' is making the cyber domain an unstable environment that is enhancing the risk of slipping from operations that hitherto have been treated as falling below the 'armed conflict' threshold to those that are or are *perceived* to cross that threshold and thus governed by international humanitarian law. That said, where that threshold lies remains contested and often murky despite attempts to substitute politics with law and subjective with objective criteria. Although there seems to be little doubt that a cyber operation alone can bring into operation international humanitarian law, under what circumstances this could happen remains contested.[10] This is not merely a matter of theoretical or even scholarly debate. What bodies of law apply to a given situation of violence is critical to assessing what norms apply and to whom not only to remind State and non-State actors of their legal responsibilities but to hold them responsible for non-compliance.[11] That is the *minimum* that survivors and victims of all forms of violence, including the violence of armed conflict, deserve.[12]

2. CLASSIFICATION AND SOVEREIGNTY

In this chapter I explore two features of cyber operations – their effects and spatial scope – both of which are pertinent to classification. By effects, I refer to the material consequences that can result from cyber operations which are requiring us to revisit well-established treaty and customary international law rules about precisely what harm international humanitarian law seeks to protect against and why.[13] By spatial scope, I refer to the fact that cyber operations are more likely than not to contain a transborder element which means that traditional interpretations of the law that assume a territorial link are no longer tenable. More importantly, I see efforts to retain a nexus between classification and geography as being counter-productive and, if anything, such an approach risks undermining the protections that international humanitarian law may offer.[14]

---

critical civilian infrastructure. See, e.g., https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

[10] See Tallinn Manual (n 5) rule 82 and its commentary. See also ICRC, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd edn, 2016, para 245 (hereinafter Commentary on the First Geneva Convention); and ICRC, *Commentary on the Second Geneva Convention: Convention (II) for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea*, 2nd edn, 2017, para 276 (hereinafter Commentary on the Second Geneva Convention).

[11] This includes not only criminal responsibility but State responsibility and full and meaningful reparations for all rights violations.

[12] Thus, deeply embedded in the seemingly dispassionate legalistic formulae to conflict classification is an ethical commitment to those who the law attempts to protect amidst the irrationality of violence and war.

[13] Contemporary international humanitarian law is founded on two rationales that are always in tension – State security and human security. Although legal experts often speak of the 'balance' between humanitarianism and military necessity, this is not an accurate account of how the law operates.

[14] This same argument holds true for international human rights law; see Louise Arimatsu, *The Geography of International Law and the Cyber Domain*, Oxford Human Rights Hub (25 February 2015) http://ohrh.law.ox.ac.uk/the-geography-of-international-law-and-the-cyber-domain/.

The history of classification and reasons for why States still insist on distinguishing between different types of armed conflict as a matter of international law has generated a rich body of scholarship.[15] Many of these accounts trace the legal distinction between international and non-international armed conflicts to international law's history and to the political interests of States. As this scholarship shows, the distinction originated in the early years of international law at a time when war was conceived as 'the contention between two or more States through their armed forces for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases'.[16] Framed by this view, classical international law was concerned primarily, if not exclusively, with regulating inter-State relations. Accordingly, what would come to be known as international humanitarian law, simply had no place in regulating intra-State violence save through the recognition of insurgency or belligerency or by way of ad hoc agreements between the warring parties. In parallel, the regulation of intra-State violence was regarded as governed by domestic law justified and normalized through the doctrine of State sovereignty, enabling the politically constructed State to reaffirm a monopoly over legitimate violence within its territory.[17] In short, it was international law's *silence* that shaped the intellectual foundations for the distinction to take root. The adoption of the 1949 Geneva Conventions which extended the reach of international humanitarian law to internal conflict through Common Article 3 (CA 3) thus marked a fundamental turning point. While this move corresponded with the radical re-conceptualization of international law exemplified by the advent of international human rights law, CA 3 was ground-breaking in that it was the first codified limitation on sovereignty agreed to by States, albeit reluctantly. This reluctance gave rise to two significant legal consequences that remain relevant today: the bifurcation of international humanitarian law and the codified setting of a higher threshold for the applicability of international humanitarian law to internal conflict.

Four 'categories' of armed conflict are now recognized under treaty law: i) international armed conflict, or those waged between two or more States; ii) international armed conflict involving national liberation movements; iii) non-international armed conflict, which include both those fought between the armed forces of the State and an organized non-State

---

[15] On classification generally, see Sylvain Vité, 'Typology of Armed Conflicts in International Humanitarian Law: Legal Concepts and Actual Situations' (2009) 91 *Intl Rev of the Red Cross* 69; Dapo Akande, 'Classification of Armed Conflicts: Relevant Legal Concepts' in Elizabeth Wilmshurst (ed), *International Law and the Classification of Conflicts* (OUP 2012); *Classification of Conflicts: Syria, Yemen and Libya*, Chatham House Report (2014); Michael N Schmitt, 'Classification of Cyber Conflict' (2012) 17 *J of Conflict and Security L* 245; Marko Milanovic and Vidan Hadzi-Vidanovic, 'A Taxonomy of Armed Conflict' in Nigel D White and Christian Henderson (eds), *Research Handbook on International Conflict and Security Law: Jus ad Bellum, Jus in Bello and Jus post Bellum* (Edward Elgar 2013) 256–314.

[16] Lassa Francis Oppenheim, *International Law: A Treatise*, Volume II (Longmans 1944) para 54. Although it is common to speak of a 'right' of States to wage war, as Oppenheim notes, 'it turns out to be no right at all, as there is no corresponding duty in those against whom the right is said to exist'; para 74.

[17] As Weber elaborates:

> the state is the form of human community that … lays claim to the monopoly of legitimate physical violence within a particular territory… all other organizations or individuals can assert the right to use physical violence only insofar as the state permits them to do so. The state is regarded as the sole source of the 'right' to use violence

Max Weber, *Vocation Lectures* (Hackett Publishing Company 2004) 33.

armed group or between such groups; and iv) non-international armed conflict regulated by Additional Protocol II.[18] The second and fourth categories are relevant only to Parties to Additional Protocol I and II, while the first and third categories, which are codified in Common Articles 2 and 3 of the Geneva Conventions and reaffirmed in subsequent treaties and State practice, are customary categories.[19] Identifying the character of the conflict is necessary because the threshold for the applicability of international humanitarian law differs between international and non-international armed conflict *and* different rules apply depending on the type of armed conflict.[20]

Insofar as the codified law is concerned, 'the differences are vast'.[21] The principle treaties governing international armed conflicts include the 1949 Geneva Conventions, Additional Protocol I of 1977 and the Regulations annexed to the Fourth Hague Convention of 1907. By contrast, the treaty rules applicable to non-international armed conflicts are limited to Common Article 3 of the 1949 Geneva Conventions and Additional Protocol II of 1977. That said, the legal chasm that once distinguished international armed conflict from non-international armed conflict no longer holds true today. Since the mid-1990s States have embraced the extension of many of the rules applicable in international armed conflict to non-international armed conflict.[22] In part this is evidenced by the extension of a number of weapons treaties to non-international armed conflict; but it has been the evolution of customary international law that has been game-changing.[23] Consequently, there is now broad agreement that as far as the rules pertaining to the conduct of hostilities are concerned, the type of conflict being fought matters little. However, the rules diverge significantly in regard to the status of the parties to the conflict. In the case of international armed conflict, combatants are entitled to combat immunity and other supplementary rights principally in the context of detention as set forth in treaty and customary international law. In contrast, the concept of combat immunity is not known in non-international armed conflict. The consequence of this is that domestic law will determine whether or not those who use force are doing so lawfully; those without lawful authority to do so will be subject to domestic criminal law. Since it is unlikely that States will ever agree to a complete abolition of the distinction (after all, to do so would be to strip the

---

[18] ICRC, 'How is the term "Armed Conflict" defined in international humanitarian law?' (Opinion Paper, March 2008) http://www.icrc.org/eng/resources/documents/article/other/armed-conflict-article-170308.htm.

[19] Commentary on the First Geneva Convention (n 10) para 193.

[20] The types of conduct that are criminalised also differs exemplified by the Rome Statute of the International Criminal Court that lists 14 offences which only apply in international armed conflict.

[21] Akande (n 15) 34.

[22] See e.g., Sandesh Sivakumaran, 'Re-envisaging the International Law of Internal Armed Conflict' (2011) 22 *European Journal of International Law* 219, 222–36.

[23] In the case of *Tadić*, the ICTY held that:

> it cannot be denied that customary rules have developed to govern internal strife. These rules ... cover such areas as protection of civilians from hostilities, in particular from indiscriminate attacks, protection of civilian objects, in particular cultural property, protection of all those who do not (or no longer) take active part in hostilities, as well as prohibition of means of warfare proscribed in international armed conflicts and ban of certain methods of conducting hostilities

Prosecutor v. Dusko Tadić, Appeals Chamber Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, Case No. IT-94-1-AR72 (2 October 1995) para 127 (hereinafter Tadić Appeals Chamber Decision). See also Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law Study* (CUP 2005).

State of its very essence), classifying the conflict – or identifying the type of conflict to which the particular situation of violence amounts – will remain a critical issue for the foreseeable future.[24]

It is often suggested that recent wars, from those in the Balkans to the conflict with Al-Qaeda and ISIS, have disrupted the clear distinction between the two types of conflict, making classification even more difficult.[25] But even a cursory review of history seems to cast doubt on this view since most conflicts, albeit to different degrees, have typically been characterized by the involvement of multiple actors, States and organized armed groups. What has changed is the extent to which wars are now viewed through the prism of the law including international criminal law and international human rights law, both of which apply concurrently with international humanitarian law. The normative and institutional advancements of international criminal law and international human rights law coupled with the need for legal coherency in how these regimes interact, nevertheless, has exposed the shortcomings of international humanitarian law in its codified form as well as the assumptions upon which it is constituted that do not necessarily reflect the complex realities on the ground nor indeed in the cyber domain.

2.1 International Armed Conflict

As set forth in Common Article 2 to the Geneva Conventions, an international armed conflict exists in 'all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them'.[26] In the absence of a treaty definition of 'armed conflict', the seemingly innocuous but pivotal question that has long dominated discussions is 'when does an armed conflict exist between States to operationalize international humanitarian law?' The Pictet commentary offers some guidance with the statement that '[a]ny difference arising between two States and leading to the intervention of armed forces is an armed conflict within the meaning of Article 2… It makes no difference how long the conflict lasts, or how much slaughter takes

---

[24] The fear of legitimizing non-State armed groups is incorporated into Common Article 3, which declares that its application 'shall not affect the legal status of the Parties to the conflict'.

[25] Some commentators have suggested that these conflicts have given rise to a new category of 'transnational armed conflict'. See, e.g., Geoffrey S Corn, 'Hamdan, Lebanon, and the Regulation of Armed Conflict: The Need to Recognize a Hybrid Category of Armed Conflict' (2006) 40 *Vanderbilt Transnational L J* 295; Geoffrey S Corn and Eric T Jensen, 'Untying the Gordian Knot: A Proposal for Determining Applicability of the Laws of War to the War on Terror' (2008) 81 *Temple L Rev* 787; Geoffrey S Corn, 'Making the Case for Conflict Bifurcation in Afghanistan' (2009) 85 *Intl L Studies* 181.

[26] Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (12 August 1949) 6 UST 3114, 75 UNTS 31; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (12 August 1949) 6 UST 3217, 75 UNTS 85; Convention Relative to the Treatment of Prisoners of War, 12 August 1949, 6 UST 3316, 75 UNTS 135; Convention Relative to the Protection of Civilian Persons in Time of War, 12 August 1949, 6 UST 3516, 75 UNTS 287. Art 2 also recognised situations of 'partial or total occupation' to constitute international armed conflict. For States Party to Additional Protocol I, wars of national liberation or 'armed conflicts in which peoples are fighting against colonial domination, alien occupation, or racist regimes in the exercise of their right of self-determination' are to be considered international armed conflicts; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (8 June 1977) 1125 UNTS 3 Art 1(4).

place'.[27] Discussions on the contours of what constitutes 'armed conflict' have been further enrichened by international criminal law. The declaration by the Appeals Chamber of the ICTY in *Tadić* case – extrapolated from Common Article 2 – that an international armed conflict exists 'whenever there is a resort to armed force between States' has reformulated the question prompting a wealth of exchanges around two issues: i) what constitutes 'armed force', a jurisprudential creation that is not defined in IHL; and ii) what conduct is attributable to a State.[28] This has arguably broadened the legal debate galvanizing experts to draw on multiple intersecting bodies of law to develop a more contextual understanding of armed conflict including in the cyber domain.

(a) The use of 'armed force'

Orthodox conceptions as to what constitutes 'armed force' assume that physical force in one shape or another is exercised principally through the use of conventional weapons that release kinetic force. To the extent that cyber operations do not entail the use of force as traditionally conceived (after all they are nothing other than a collection of codes) but, nonetheless, are quite capable of producing destructive or deadly results analogous to conventional means and methods of warfare, attention has shifted to the *effects* of such operations. As Droege describes, 'if a computer network attack causes airplanes or trains to collide, resulting in death or injury, or widespread flooding with large-scale consequences, there would be little reason to treat the situation differently from equivalent attacks conducted through kinetic means or methods of warfare'.[29] Few would disagree that the scenarios depicted by Droege would satisfy the criterion of 'armed force' triggering the applicability of international humanitarian law.[30] The effects described are not only violent but severe and certainly fall squarely within what constitutes an attack within the meaning of Article 49(1) of Additional Protocol I.[31] This

---

[27] Jean Pictet (ed), *Commentary to the First Geneva Convention for the Amelioration of the Condition of the Wounded and the Sick in Armed Forces in the Field* (1952); Geneva Convention II (1960); Geneva Convention III (1960); Geneva Convention IV (1958). The drafters were concerned with emphasizing the *de facto* nature of the hostilities over official characterizations as a way to privilege law over politics and international over domestic law.

[28] Tadić Appeals Chamber Decision (n 23) para 70. This statement is now regarded as being reflective of customary international law.

[29] Cordula Droege, 'Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94 *Intl Rev of the Red Cross* 533, 546. This understanding is consistent with the views expressed by the drafters of the 2016 ICRC Commentary to Art 2, Geneva Convention I, which explains that:

> it is generally accepted that cyber operations having similar effects to classic kinetic operations would amount to an international armed conflict. Indeed, if these operations result in the destruction of civilian or military assets or cause the death or injury of soldiers or civilians, there would be no reason to treat the situation differently from equivalent attacks conducted through more traditional means and methods of warfare

Commentary on the First Geneva Convention (n 10) para 255.

[30] Ibid., para 255 and Commentary on the Second Geneva Convention (n 10) para 277. The Commentary also clarifies that 'any attack directed against the territory, population, or the military or civilian infrastructure constitutes a resort to armed force against the State to which this territory, population or infrastructure belongs', para 246. See also Tallinn Manual (n 5) rule 92.

[31] Art 49(1) of Additional Protocol I define attacks as 'acts of violence against the adversary, whether in offence or defence'. Used in an operational sense, 'cyber operations' refer to the employment of cyber capabilities to achieve objectives in or through cyber space and include 'cyber attacks' which are specif-

had led most experts to reason that all cyber-attacks, within the meaning of Article 49(1), by a State against another would activate an international armed conflict.

Over the last decade, there has been much debate around what constitutes a cyber-attack not only within the context of an existing armed conflict but also because an attack would 'signpost' the existence of an armed conflict. The prevailing view is that cyber operations constitute attacks when they are reasonably expected to or result in 'death or injury of individuals, whether civilians or combatants, or [physical] damage to or destruction of objects, whether military objectives or civilian objects'.[32] Of course, the nature of cyber-attacks are such that they invite us to revisit traditional assumptions around causation since, in contrast to attacks involving conventional weapons where material violence is caused directly, cyber-attacks are by definition always at a minimum one step removed from the resulting material violence.[33] This is captured by the ICRC's position that a cyber-attack 'includes harm due to the foreseeable direct and indirect (or reverberating) effects of an attack, for example the death of patients in intensive-care units caused by a cyber operation on an electricity network that results in cutting off a hospital's electricity supply'.[34] While hugely compelling, to define an attack by reference to the indirect effects of the operation is also potentially problematic in that it opens up the possibility that the manipulation of the financial system would constitute 'armed force' since death and injury, at least for some, are inevitable outcomes of economic and/or financial loss.[35] In other words, what the cyber domain is forcing us to recognize is that all law, including international humanitarian law, is often founded on arbitrary distinctions and temporal assumptions. If a cyber-attack is indeed the marker for the existence of an armed conflict, the problem with the above construction is that it provides little insight on how severe the violent effects must be to constitute 'armed force'.[36] Nor does it fully capture the uncertainty over what damage to objects entails in the cyber realm. Consequently, it risks being both over- and under-inclusive.[37]

Legal experts continue to differ over the 'threshold of violence' question for good reason. The jurisprudence of the ICTY would suggest that the threshold is very low indeed and that nearly any use of 'armed force' would suffice save those that are the result of mistake.[38] This

---

ically designed operations to disrupt, deny, degrade or destroy information in computers and computer networks, or the hardware itself and/or to affect the physical systems that rely on digital technologies to operate.

[32] For example, Schmitt (n 15) 245–260, 251; Knut Dörmann, 'Applicability of the Additional Protocols to computer network attacks' (ICRC 2004); Nils Melzer, 'Cyberwarfare and international law' (UNIDIR Resources Paper 2011); Tallinn Manual (n 5) rule 92.

[33] Cyber-attacks are codes directed at other digital systems or networks that may or may not have control over a tangible object. The code may cause failure or damage to the hardware component or cause the digital system that controls the object to malfunction. For a useful insight into causes and effects see Glenn Shafer, 'Causality and Responsibility' (2000) 22 *Cardozo L Rev* 1811.

[34] ICRC Position Paper (n 5) 7.

[35] This is not to suggest indirect effects are not relevant since clearly they are; the problem is where one draws the line.

[36] The objective of Art 49 is not to provide the test/barometer for the existence of an armed conflict but rather to define 'attacks' and their scope of application.

[37] Michael N Schmitt, 'Cyber Operations and the Jus in Bello: Key Issues' (2010) 87 *International Law Studies* 89, 94.

[38] Commentary on the First Geneva Convention (n 10) para 241; Commentary on the Second Geneva Convention (n 10) para 263.

comports with the position taken by the ICRC which, as would be expected, has consistently urged for a low threshold to ensure maximum protection for those whom the Conventions aim to protect.[39] The ICRC's 2016 *Commentary* maintains that no 'specific level of violence' is required to trigger the application of the Conventions[40] and goes even further by suggesting that 'any unconsented-to military operations by one State in the territory of another State should be interpreted as an armed interference in the latter's sphere of sovereignty and thus may be an international armed conflict under Article 2(1)'.[41] If this is indeed an accurate interpretation of existing law, there is a persuasive case to be made that many of the cyber operations that have been and are being conducted by States are governed by international humanitarian law, notwithstanding State silence to support such a conclusion.[42] That said, the relationship between law and practice seems to almost unravel in the cyber domain. In a digital age when State power is no longer confined to physical presence nor for that matter to any level of control, it may be that analogies simply do not apply.

Those who maintain that the hostilities must reach a certain level of intensity (and/or duration) before an armed conflict exists generally do so based on State practice as well as concerns over international humanitarian law's more permissive rules on the use of force becoming the default option.[43] Evidence of the former is not hard to find. Over the years, there have been numerous incidents involving the use of armed force between States that have resulted in death, injury and considerable destruction and damage to property, yet been described as 'sporadic border clashes' or naval 'incidents' rather than armed conflict. That said, the practice

---

[39] See also Claude Pilloud and others (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC/Martinus Nijhoff 1987) para 62. In the absence of any other international legal regime offering protection, this argument is a persuasive one. However, the concurrent applicability of international human rights law means that international humanitarian law is no longer the only legal regime that applies in times of armed conflict. The 2016 Commentary urges that 'once States start using force against one another, humanitarian law provides a recognized framework to protect all those who are affected'; Commentary on the First Geneva Convention (n 10). While that may indeed be the case, there is also the need to recognize that the operationalization of international humanitarian law lowers and in some instances strips certain groups of individuals of the protections provided by international human rights law.

[40] Ibid., para 261. Although some scholars suggest that a low threshold is supported by the fact that Common Art 2 expressly recognizes the possibility for the existence of an international armed conflict without recourse to any hostilities at all: namely, for 'declared war' or 'partial or total occupation … even if said occupation meets with no armed resistance', these situations, as treaty obligations, should not be conflated with whether there is an intensity threshold in respect of 'armed conflict'.

[41] Commentary on the First Geneva Convention (n 10) para 237; Commentary on the Second Geneva Convention (n 10) para 245. For concise summary of distinction between 'military operations' and 'attacks' in the cyber context, see Rain Liivoja, Kobi Leins and Tim McCormack, 'Emerging Technologies of Warfare' in Rain Liivoja and Tim McCormack (eds), *Routledge Handbook of the Law of Armed Conflict* (Routledge 2016) 608–9.

[42] Examples include the wave of wiper attacks directed against various Saudi Arabian critical economic sectors in November 2016, the cyber operations in 2017 targeting Saudi-Aramco and at least one other critical infrastructure plant both of which were designed to have destructive effects.

[43] International Law Association, *The Hague Conference: Final Report on the Meaning of Armed Conflict in International Law* (2010). The argument that having an intensity threshold would create a legal protection vacuum is not entirely compelling since this rests on the assumption that no other body of international law is applicable. For the humanitarian, the desire to claim maximum protection whilst restricting the use of force by States is the unresolvable paradox presented by international humanitarian law.

of States has been mixed.[44] By and large, the denial by States as to the existence of a conflict are the result of political calculations including very real concerns over the potential escalation of hostilities, not least in the cyber domain.

To date, no known hostile cyber operation has resulted in human casualties and only in a few instances have attacks resulted in physical damage whether to digital hardware or to objects that operate on digital technologies. However, even in situations where physical damage has been caused *and* there is evidence to show that the operation was orchestrated by another State, States have shown little appetite to claim the hostile cyber operation as tantamount to triggering an armed conflict.[45] Does this mean that in the cyber realm the severity of the violent consequences, especially if the damage to property is treated as a temporary set-back, albeit costly, does matter?[46] In other words, does it necessarily follow that *all* cyber-attacks operationalize international humanitarian law?

The fact that in many societies, the provision of essential services such as water, energy, communication, travel, finance and other government services including, for example, health-care and the emergency services are now reliant on a 'vast array of interdependent information technology (IT) networks, systems, services, and resources' and that cyber operations can cause considerable harm without necessarily causing physical damage to cyber infrastructure has led to a reappraisal of what constitutes damage under international humanitarian law.[47]

---

[44] In situations where members of the armed forces have been detained, States have claimed the applicability of the Conventions, irrespective of the level of hostilities in order that the members of their armed forces can benefit from the protections afforded by combat immunity and POW status. For example, in 1982, the US demanded that a Navy pilot shot down by Syrian armed forces in the Bekaa Valley, Lebanon, be treated as a POW. Likewise, in 1998, the US demanded that US forces captured in Macedonia by Serbia be extended POW status. However, in contrast, the Conventions were not invoked by either the UK or US following the detention by Iran of British sailors in 2007 and the crew of a US Navy patrol boat in 2015. In the case of the UK, there is evidence to suggest that Consular access was demanded suggesting that domestic law was relevant. An alternative approach is to suggest that situations involving detention should be treated as the exception to the rule. For further analyses see also Christopher Greenwood, 'Scope of Application of Humanitarian Law' in Dieter Fleck (ed), *The Handbook of International Humanitarian Law* (OUP 2009) 48 and Howard S Levie, 'The Status of Belligerent Personnel "Splashed" and Rescued by a Neutral in the Persian Gulf Area' (1991) 31 *Virginia J of Intl L* 611, 613–14.

[45] Notwithstanding the damage reportedly caused by the Stuxnet operation against Iran's nuclear facility at Natanz which allegedly resulted in physical destruction of about 1,000 IR-1 centrifuges Iran did not suggest that the attack activated international humanitarian law. Moreover, legal experts also remain divided on whether the Stuxnet operation triggered the application of international humanitarian law. For a useful analysis on the Stuxnet case, see Gary Brown, 'Why Iran didn't admit Stuxnet was an Attack' (2011) 63 *Joint Force Quarterly* 71. The only other known cyber-attack that has caused physical damage is in respect of a German steel mill in 2014; see Kim Zetter, 'A Cyberattack has Caused Confirmed Physical Damage for the Second Time Ever', *Wired* (8 January 2015) and Robert M Lee, Michael J Assante and Time Conway, *German Steel Mill Cyber Attack, ICS Defense Use Case (DUC)*, SANS Institute, 30 December 2014.

[46] Extensive damage to computer infrastructure, hardware and systems operating on digital technologies have not prompted States to claim the applicability of international humanitarian law. For a useful analysis see Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112 *American Journal of International Law* 583.

[47] Written testimony of NPPD Executive Order 13636 and Presidential Policy Direct 21 Integrated Task Force Director Robert Kolasky for a House Committee on Homeland Security, 'Oversight of Executive Order 13636 and Development of the Cybersecurity Framework' (18 July 2013) http://www.dhs.gov/news/2013/07/18/written-testimony-nppd-house-homeland-security-subcommittee

Most commentators take the view that 'damage' extends to the loss of functionality that renders cyber infrastructure inoperative or that necessitates repair, although opinions divide on whether loss of functionality can be temporary or must be permanent and on the nature and extent of the repair that is needed.[48]

An alternative minority view is that it is not the loss of functionality *per se* but the consequences of that loss that matters since a cyber operation that deprives a system from performing its intended function may in some circumstances simply cause inconvenience and disruption.[49] It is only when the effects of loss of functionality result in or are expected to result in death, injury, physical damage or destruction that the operation constitutes an attack. This latter view still does not explain why it is that States have not claimed the applicability of international humanitarian law following incidents in which digital systems have been disabled or the function of infrastructure or processes relying on such systems have been interfered with resulting in physical damage. The reluctance to do so is perhaps partially explained by the visceral conviction that international humanitarian law is concerned with addressing material violence of a certain severity.[50] If this is indeed the case, it would suggest that a hostile cyber operation by a State against another would have to reach a certain level of violent effects – and in cases where the severity is not substantial, duration may matter – before it is regarded as a resort to 'armed force' to trigger the application of international humanitarian law.

(b) By a state against another state

The logic of classification is premised on the fact that the identity of the adversary is known. The ability of actors to take advantage of the anonymity that cyber furnishes when conducting

---

-cybersecurity. See also ICRC, *The Potential Human Cost of Cyber Operations* (ICRC Expert Meeting 14–16 November 2018) https://www.icrc.org/en/document/potential-human-cost-cyber-operations.

[48] Michael N Schmitt, 'Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical *Vade Mecum*' (2017) 8 *Harvard National Security Journal* 239, 266. Even among experts who take this view, there is no consensus as to the nature or extent of the repair necessary; see Tallinn Manual (n 5) rule 92 and commentary. Some States, including France, e.g., appear to have adopted this interpretation of existing law; Michael N Schmitt, 'France Speaks Out on IHL and Cyber Operations: Part II' (1 October 2019) EJIL: *Talk!* https://www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-ii/.

[49] It is the effects of the attack that matter, not how it is conducted.

[50] See e.g., in 2013, the Dutch Government endorsed a report it had commissioned on cyber warfare which had concluded:

> if an organised cyber attack (or series of attacks) leads to the destruction of or substantial or long-lasting damage to computer systems managing critical military or civil infrastructure, it could conceivably be considered an armed conflict and international humanitarian law would apply. The same is true of a cyber attack that seriously damages the state's ability to perform essential tasks, causing serious and lasting harm to the economic or financial stability of that state and its people. An example would be a coordinated and organised attack on the entire computer network of the financial system (or a major part of it) leading to prolonged and large-scale disruption and instability that cannot easily be averted or alleviated by normal computer security systems.

Advisory Council on International Affairs and the Advisory Committee on Issues of Public International Law, 'Cyber Warfare 20' (No. 77, AIV/No. 22, CAVV) (December 2011) https://www.advisorycouncilinternationalaffairs.nl/documents/publications/2011/12/16/cyber-warfare and Government Response of 6 April 2012 reported in Correspondents' Reports: The Netherlands (2012) 15 *Ybk of Intl Humanitarian L*. The ICRC has taken the view that cyber operations that *disable* an object can constitute an attack, while other expert commentators have insisted on a higher threshold that is contingent on the need for physical repair to the system. See also Roscini (Ch 14 of this Handbook).

offensive cyber operations often impedes attribution which consequently presents a practical obstacle for classification. Future technological advances may minimize this problem but, as with any forensic investigation, information gathering is likely to remain time-consuming and require considerable resources.[51] Moreover, recent history suggests that disputes over attribution are likely to persist since even when persuasive evidence has been tendered indicating State involvement in a particular cyber operation or series of operations, public denial remains the dominant response.[52] The catastrophic consequences that could result as a consequence of misidentifying the source of a cyber-attack have prompted States to take some steps principally in the form of bilateral agreements to reduce this risk.[53] It should however be noted that, irrespective of whether the State is involved in the cyber operation, it is under a legal obligation not to knowingly allow its territory to be used for acts contrary to the rights of other States and must take appropriate steps to protect those rights.[54] Such obligations aside, the mere failure on the part of a State to prevent cyber-attacks from its territory – to the extent that the said attacks are not attributable to it – does not mean that an international armed conflict is triggered between it and the victim State.[55] However, a cyber operation that meets the threshold of armed force conducted without consent on the territory of another State even if directed against a non-State actor will give rise to an international armed conflict within the meaning of Common Article 2(1).[56]

---

[51] See e.g., Mandiant, 'APT1: Exposing one of China's Cyber Espionage Units' (18 February 2013) https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf, which was the outcome of a two-year investigation. But also see the statement by US Secretary of Defense Leon Panetta:

> the department has made significant advances in solving a problem that makes deterring cyber adversaries more complex: the difficulty of identifying the origins of that attack. Over the last two years, DoD has made significant investments in forensics to address this problem of attribution and we're seeing the returns on that investment. Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America

Leon E Panetta, *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City* (11 October 2012) https://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136. On cyber espionage and international law see Buchan and Navarrete (Ch 11 of this Handbook).

[52] Following the release of the report by Mandiant which contained considerable evidence to indicate State involvement in a range of cyber operations, albeit in the context of cyber espionage, the Chinese Defense Ministry countered with the statement that 'it is unprofessional and groundless to accuse the Chinese military of launching cyber attacks without any conclusive evidence'; Craig Timberg and Ellen Nakashima, 'Chinese Hackers Suspected in Attack on *The Post's* Computers', *The Washington Post* (1 February 2013) https://www.washingtonpost.com/business/technology/chinese-hackers-suspected-in-attack-on-the-posts-computers/2013/02/01/d5a44fde-6cb1-11e2-bd36-c0fe61a205f6_story.html.

[53] See Ellen Nakashima, 'U.S. and Russia Sign Pact to Create Communication Link on Cyber Security', *The Washington Post* (17 June 2013) https://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788-11e2-9df4-895344c13c30_story.html.

[54] *Corfu Channel Case (UK v. Albania)*, Judgment [1949] ICJ Rep 4, 22; *Case Concerning United States Diplomatic and Consular Staff in Tehran (USA v. Iran)* [1980] ICJ Rep 3, paras 67–8; Tallinn Manual (n 5) rules 6 and 7 and commentary.

[55] The question that remains unanswered is whether there is an international obligation on States to prevent future harmful cyber operations from being mounted once they are put on notice that further operations will be conducted from their territory.

[56] Commentary on the First Geneva Convention (n 10) paras 261–2.

To qualify as an international armed conflict, a cyber-attack on a State must be conducted by, or be ascribed to, another State. A cyber operation conducted by the armed forces of a State against another State that reaches the requisite 'armed force' threshold will trigger an international armed conflict.[57] Those conducted by other *de jure* organs of the State including law enforcement agencies and the intelligence service also qualify.[58] The pace at which advances are taking place in the cyber realm means that States are likely to bolster their capabilities by using private sector actors to exercise some governmental authority. It follows that a cyber-attack by individuals or private entities that are not organs of the State may also qualify if that person or entity has been authorized by law to perform certain governmental tasks on behalf of the State and is acting in that capacity in the particular instance.[59] However, an international armed conflict will only materialize if the cyber operation is of the type for which that person or entity has been granted legal authority to conduct.

As a general rule, an international armed conflict will *only* be activated by the actions of organs of the State or when private persons or entities are recognized as *de jure* organs of the State. However, cyber operations by private persons or entities may qualify if that person or entity is 'acting on behalf of the State' including where proxy forces are being used.[60] In other words, *de facto* organs of a State suffice. This is particularly pertinent in the cyber domain since to limit the existence of an international armed conflict to the involvement of the armed forces or indeed to private actors as defined by domestic law would 'allow States to bypass the application of humanitarian law by using non-military agencies or other surrogates not officially considered members of the armed forces'.[61]

Situations that arise with some frequency in the cyber domain is where individuals and groups that are neither organs of a State nor authorized to act on its behalf conduct cyber operations against another State as in the case of the 2007 hacktivists cyber campaign against Estonia and the more recent operations by the Ukrainian Cyber Alliance in Russia. Even if conducted in support of the State, such operations are, as a rule, not attributable to the State for the purpose of finding an international armed conflict. However, if the State formally approves

---

[57] For example, had the conflict with Libya in March 2011 to enforce UN Security Council Resolution 1973 opened with a cyber-attack by the US on Qaddafi's air-defense system (as discussed by Schmit and Shanker), the rules applicable to an international armed conflict may well have been triggered; Eric Schmitt and Thom Shanker, 'U.S. Debated Cyberwarfare in Attack Plan on Libya', *The New York Times* (17 October 2011) https://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

[58] State organs include 'any person or entity which has that status in accordance with the internal law of the State'; International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries 2001 (hereinafter Articles on State Responsibility).

[59] Ibid., Art 5 reads: 'empowered by the law of that State to exercise element of the governmental authority shall be considered an act of the State … provided the person or entity is acting that capacity in the particular instance'.

[60] *Prosecutor v Bemba*, Decision on the Confirmation of Charges, Case No. ICC-01/05-01/08 (15 June 2009) para 223. '[P]rivate individuals acting within the framework of, or in connection with, armed forces, or in collusion with State authorities may be regarded as de facto State organs', *Prosecutor v. Tadić* [1999] ICTY Appeals Chamber Judgement, IT–94–1–A, para 144 (hereinafter Tadić Appeals Chamber Judgement).

[61] Art 2, Commentary on the First Geneva Convention (n 10) para 230.

and endorses or orders the continuation of the cyber operations the persons or entity may be deemed *de facto* organs of the State and thus fulfil the 'international' criterion.[62]

It is now well-settled in international law that a conflict will be international where a State has *overall control* over a proxy or non-State organized armed group that is engaged in a conflict with another State.[63] The standard for determining such control is high in that the State must have 'a role in organising, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group'.[64] The provision of cyber tools – whether in the form of software or hardware – by a State to an organized armed group together with the supply of specific intelligence on cyber vulnerabilities of the 'victim' State to facilitate a particular attack may suffice for the purpose of classifying the conflict as international.[65] Courts and tribunals have taken a different view in respect of persons or groups not organized into military structures. In such circumstances, rather than overall control, there must be 'specific instructions or directives aimed at the commission of specific acts' for the purpose of classifying the conflict as international.[66] It would follow that if an individual hacker or a group of hacktivists were to conduct a cyber-attack on the specific instructions of a State they would be regarded as *de facto* State organs and the attack would be treated as if launched by *de jure* State organs for the purpose of classifying the conflict as international.[67]

---

[62] Tadić Appeals Chamber Judgement (n 60) 133, 137. This principle can be traced to the judgment of the International Court of Justice in the *Case Concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgment (Merits) [1980] ICJ Rep 14, although the principle was formulated in the context of State responsibility.

[63] Tadić Appeals Chamber Judgement (n 60) paras 131–40, 145. According to the tribunal:

> control by a State over subordinate armed forces or militias or paramilitary units may be of an overall character (and must comprise more than the mere provision of financial assistance or military equipment or training). This requirement, however, does not go so far as to include the issuing of specific orders by the State, or its direction of each individual operation. Under international law it is by no means necessary that the controlling authorities should plan all the operations of the units dependent on them, choose their targets, or give specific instructions concerning the conduct of military operations and any alleged violations of international humanitarian law. The control required by international law may be deemed to exist when a State (or, in the context of an armed conflict, the Party to the conflict) has a role in organising, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group.

The International Court of Justice has noted that that the 'overall control' is 'applicable and suitable' for the purpose of determining whether or not an armed conflict is international; *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* [2007] ICJ Rep 43, para 404. See also ICC, Lubanga Trial Judgement, 2012, para 541 and Bemba Trial Judgment, 2016, para 130 and Commentary on the First Geneva Convention (n 10) paras 270–3.

[64] Tadić Appeals Chamber Judgement (n 60) paras 137, 145. The standard for attribution of State responsibility – complete dependency and effective control – is however higher.

[65] Tallinn Manual (n 5) Commentary to rule 82, para 6.

[66] Tadić Appeals Chamber Judgement para 132 (n 60). See also Art 8 of the Articles on State Responsibility, which permits attribution 'if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct'; Articles on State Responsibility (n 58).

[67] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA)* (Merits, Judgment) [1986] ICJ Rep 14. It should be noted that the 'effective control' test evolved in the context

2.2 Non-international Armed Conflict

As with international armed conflict, there is no codified definition of what constitutes a non-international armed conflict. Common Article 3 to the Geneva Conventions defines non-international armed conflicts in the negative as those that are 'not of an international character occurring in the territory of one of the High Contracting Parties'.[68] Treaty law also informs us as to what type of violence is *not* governed by international humanitarian law. Article 1(2) of Additional Protocol II, which is acknowledged to represent customary international law, excludes situations of 'internal disturbances and tensions, such as riots, isolated and sporadic acts of violence, and other acts of a similar nature'.[69] This threshold also applies to Common Article 3. What we can safely conclude from this is that isolated and sporadic cyber-attacks – even if they lead to death, injury, damage and destruction – may not necessarily be governed by international humanitarian law since to qualify as a non-international armed conflict the level of violence must cross a threshold above those situations described in Additional Protocol II.[70]

Of equal pertinence is the reference in Additional Protocol II that describes such conflicts as those between a State's armed forces 'and dissident armed force or other organized armed groups'.[71] Elaborating on these provisions, the ICTY's portrayal of a non-international armed conflict as 'protracted armed violence between governmental authorities and organized armed groups or between such groups within a State' is now regarded as customary international law.[72] Accordingly, the existence of a non-international armed conflict is contingent on two key elements: (i) the involvement of an organized armed group; and (ii) the hostilities reaching a certain level of intensity.[73] As the ICTY has repeatedly emphasized, the two determinative elements of an armed conflict function 'solely for the purpose, as a minimum, of distinguish-

---

finding State responsibility for the acts of non-State actors. See *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (n 63).

[68] Although not in the text, it has always been assumed that the provision applies to hostilities between government forces and armed groups as well as between such groups. See Pilloud (n 39) para 4461.

[69] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts (n 26). Further insight is provided in Pilloud (n 39), which adds 'riots, such as demonstrations without a concerted plan from the outset; isolated and sporadic acts of violence, as opposed to military operations carried out by armed forces or armed groups; other acts of a similar nature, including, in particular, large scale arrests of people for their activities or opinions' (para 4474).

[70] Prior to the adoption of the Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts (n 26) there was already widespread agreement that the existence of a non-international armed conflict requires 'open hostilities between armed forces which are organized to a greater or lesser degree' (Pilloud (n 39) para 4341).

[71] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts (n 26) art 1(1).

[72] This formula has also been applied by the International Tribunal for Rwanda, the Special Court for Sierra Leone and the International Criminal Court among others.

[73] Tadić Appeals Chamber Decision (n 23) para 70. There are two types of non-international armed conflict. All non-international armed conflicts are covered by common art 3 to the Geneva Conventions; in addition, the provisions of Additional Protocol II, which sets forth far more detailed rules, apply to non-international armed conflicts fulfilling the additional criteria set forth in art 1(1) but only in respect of States Parties to that Protocol.

ing an armed conflict from banditry, unorganized and short-lived insurrections, or terrorist activities, which are not subject to international humanitarian law.'[74]

Before examining how these two criteria might apply in the cyber context, some mention of the recent debates pertaining to the geographical scope of non-international armed conflict is apposite. This is because cyber operations are more likely than not to cross borders reigniting disagreements as to whether Common Article 3 incorporates a spatial element limiting the geographical scope of non-international armed conflicts. One view insists that, by definition, such conflicts are those waged exclusively within the territorial boundaries of a single State, and so, by default, those that cross a border are necessarily international in character. Taken to its logical conclusion, a cyber-operation conducted from outside the territory would internationalize the conflict. A second view, and one shared by the majority of commentators, holds that the word 'one' in the text refers to the territory of any of the Contracting Parties and therefore the phrase does not impose a territorial limitation. Accordingly, a cyber-operation mounted by either party to the conflict from outside the territory would not alter the character of the conflict. The consequence of this view is that non-international armed conflict, because defined solely by the parties to the conflict rather than the location, has the potential to be global in scope.[75] This has caused anguish among some within the international legal community who, in seeking to limit the scope of sovereign power, have strenuously argued for rigid adherence to a catalogue of legal tests both in regard to *jus in bello* and *jus ad bellum*.[76]

(a) The involvement of an organized armed group

The element of organization represents the principle that an armed conflict can exist only between parties that are sufficiently organized to confront each other with military means.[77] State authorities are presumed to have at their disposal armed forces that satisfy this criterion but the same assumption cannot be made of an armed group which, by contrast, must demonstrate that it does indeed fulfil this requirement. The armed group does not have to have an organization structure of a conventional military unit. As the ICTY has noted 'some degree of organisation by the parties will suffice'.[78] Whether a group is deemed to be 'organized' is a factual question and, as repeatedly emphasized by the tribunal, it is an assessment that is always context-specific. To enable that assessment, a variety of indicators have been identified including, for example, the organization and structure of the armed group; the adoption of internal regulations; the capacity to launch coordinated military operations; and the capacity

---

[74] Tadić Appeals Chamber Judgement (n 60) para 562.

[75] See Louise Arimatsu, 'Territory, Boundaries and the Law of Armed Conflict' (2009) 12 *Yearbook of Intl Humanitarian L* 157; Michael N Schmitt, 'Charting the Legal Geography of Non-International Armed Conflict' (2014) 90 *Intl Law Studies* 1.

[76] See, e.g., Noam Lubell and Nathan Derejko, 'A Global Battlefield?' (2013) 11 *J of Intl Criminal Justice* 65 and Philip Alston, 'The CIA and Targeted Killings Beyond Borders' (2011) 2 *Harvard National Security J* 283. For a different viewpoint see Robert Chesney, 'Who May Be Killed? Anwar al-Awlaki as a case study in the international legal regulation of lethal force' (2010) 13 *Yearbook of Intl Humanitarian L* 360 and Ashley Deeks, 'The Geography of Cyber Conflict: Through a glass darkly' (2013) 89 *Intl L Studies* 1.

[77] *Prosecutor v. Ramush Haradinaj, Idriz Balaj, Lahi Brahimaj* (Judgement) [2008] Case No. IT-04-84-T, para 60.

[78] *Prosecutor v. Fatmir Limaj, Haradin Bala, Isak Musliu* (Judgement) (2005) Case No. IT-03-66-T, para 89.

to provide military training.[79] While none of the indicators are essential in and of themselves to establish whether the organization criterion is fulfilled,[80] what is clear is that the lone hacker or even groups of hackers sympathetic to a common cause and acting collectively but not as a coordinated entity would simply not qualify on the basis that they are operating independently of one another.[81]

This raises the question of whether a 'virtual group' – in other words, a group that is organized exclusively on-line – would qualify. The capacity to launch coordinated military operations together with the ability to impose discipline are characteristics often cited as necessary to qualify as an organized armed group.[82] Insofar as the former element is concerned, there is no reason why an on-line group would not be able to 'act in a coordinated manner against the government (or an organized armed group), take orders from a virtual leadership, and be highly organized'.[83] Existing on-line groups have frequently demonstrated an ability to plan and carry out cyber operations in a coordinated manner directed by a leadership although none of the operations, to date, can be equated to 'armed force'.[84] In short, there is no reason why a virtual group could not carry out cyber operations on a par with 'sustained and concerted military operations' and so satisfy the requisite threshold.[85] Nevertheless, most commentators have dismissed the prospect that such groups can qualify on the basis that groups formed and acting exclusively on-line would be unable to enforce discipline and the observation of international humanitarian law.[86] Yet is such a conclusion warranted? This scepticism is commonly justified on the grounds that the group would lack 'physical control over its members'.[87] This raises a number of questions. Is physical control a pre-condition to discipline and rule enforcement? Does the law, as drafted, presuppose physical control precluding its applicability to virtual groups or should a distinction be drawn between Additional Protocol II and Common Article 3 conflicts?

---

[79] Other criteria identified by the ICTY include, the nomination of a spokesperson; the issuing of orders, political statements and communiqués; the establishment of headquarters; the establishment of a military police and disciplinary rules; the ability to recruit new members; the creation of weapons distribution channels; the use of uniforms and various other equipment; and the participation by members of the group in political negotiations.

[80] *Prosecutor v. Ramush Haradinaj, Idriz Balaj, Lahi Brahimaj* (n 77) para 60.

[81] As the commentary to rule 83 of the Tallinn Manual (n 5) notes:
> the mere fact that individuals are acting toward a collective goal does not satisfy the organization criterion. For example, if a website makes available malware and provides a list of potential cyber targets, those who independently use the site to conduct attacks would not constitute an organized armed group.

[82] The organizational element is satisfied when the group in question operates 'under an established command structure and has the capability to sustain military operations'; Tallinn Manual (n 5) rule 83, para 11.

[83] Schmitt (n 15) 256.

[84] It is common practice for the leadership of such groups to publicly declare their intentions and reasons for a particular cyber operation; issue information on planned actions and execution dates through video, social media announcements, and pastebin entries; release lists of targets; provide tools to execute the operation.

[85] Pilloud (n 39) para 4453.

[86] It should be recalled that the 'International Group of Experts [involved in the preparation of the Tallinn Manual] was divided as to whether such difficulty would bar qualification as an organized armed group'; Tallinn Manual (n 5) commentary to rule 83.

[87] Schmitt (n 15) 257.

An express reference to the capacity of an organized group to enforce international humanitarian law only appears in Additional Protocol II which applies:

> to all armed conflicts which are not covered by Article 1 of [Additional Protocol I] and which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol.[88]

The requirement in the text that the organized armed group *implement this Protocol* is generally accepted as an ability to comply with international humanitarian law. What matters is that the organized armed group is *capable* of enforcing the rules rather than whether it does so or not.[89] Insofar as Additional Protocol II conflicts are concerned, it is clear from the text that the capacity to enforce is a necessary criterion of organization as is the existence of a responsible command and the ability to carry out sustained and concerted military operations.[90] What is also apparent from the jurisprudence of the international tribunals is that evidence in support of such a capacity is more often than not equated to an ability to exert physical control over persons.[91] Nevertheless, whether the capacity to enforce is always contingent on physical control is a matter of debate since why individuals comply with a rule is a complex matter and may not necessarily be dependent on the threat of a sanction in the form of physical force but, for example, on the threat of exclusion from the group as well as 'exposure' of their identity to the authorities by group members.[92]

Even if absence of physical contact is not a bar to qualification, a closer inspection of the law presents a further hurdle. Although the virtual organized armed group might be capable of enforcing discipline amongst its members and insist on adherence to the rules pertaining to the conduct of hostilities as a condition of membership, it is an inescapable fact that the group would lack the capacity to implement those rules concerned with protecting the victims of conflict which arguably represent the very *raison d'être* of both Common Article 3 and Protocol II. The very characteristic of the group precludes it from, for example, caring for the wounded and the sick, making particular provisions for children, or ensuring that detainees were treated humanely simply because the members would never have any physical contact with one another let alone with any victims of the hostilities.[93] Thus the virtual group presents a particular problem in that, as traditionally understood, the law does presuppose some degree of physical contact. Does this mean that international humanitarian law can *never* apply to the conduct of a virtual group?

---

[88] Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of Non-international Armed Conflicts (n 26) art 1.

[89] *Prosecutor v. Ljube Boškoski Johan Tarčulovski* (Judgement) [2008] Case No. IT-04-82-T para 205.

[90] Pilloud (n 39) para 4453.

[91] *Prosecutor v. Fatmir Limaj, Haradin Bala, Isak Musliu* (n 78) paras 114–117.

[92] Douglas Heckathorn, 'Collective Sanctions and Compliance Norms: A formal theory of group-mediated social control' (1990) 55 *American Sociological Rev* 366; Karen Cook and Russell Hardin, 'Norms of Cooperativeness and Networks of Trust in Social Norms' in Michael Hechter and Karl-Dieter Opp (eds), *Social Norms* (Russell Sage Foundation 2001) 327.

[93] Pilloud (n 39) para 4426.

In contrast to Additional Protocol II, Common Article 3 contains no analogous express condition as constituting a requirement of qualification. As the Commentary to Article 3 notes, the capacity of an organized armed group to respect and ensure respect for international humanitarian law was one among a number of criteria considered and *rejected* by the Diplomatic Conference that drafted the 1949 Geneva Conventions. Moreover, the Commentary further emphasizes that none of the conditions that were considered are 'obligatory and are only mentioned as an indication'.[94] Admittedly, in assessing the organization of an armed group, the ICTY has, when appropriate, taken into consideration the 'level of discipline and the ability to implement the basic obligations of Common Article 3 … such as the establishment of disciplinary rules and mechanisms; proper training; and the existence of internal regulations and whether these are effectively disseminated to members'.[95] However, the tribunals have also conceded that 'none of [the criteria, including the ability to implement the law] are, in themselves, essential to establish whether the 'organization' criterion is fulfilled'.[96] This would suggest that no such mandatory condition applies to Common Article 3 conflicts. While this view may provoke disagreement, perhaps the most compelling reason for not rejecting the possibility of Common Article 3 applying to a virtual group is that the consequences of excluding such groups would potentially be counter-productive. As the drafters of the Commentary to Common Article 3 strenuously maintained, 'the Article should be applied as widely as possible' for the very simple reason that the overriding objective of the provision is to protect the victims of conflict.

(b) The intensity of the hostilities

Unlike international armed conflict, the hostilities between the parties must reach a certain level of intensity before a non-international armed conflict is deemed to exist. The ICTY has identified various indicative criteria to facilitate the determination as to whether a given situation has met the required intensity threshold. Examples include the gravity of attacks and their recurrence;[97] the temporal and territorial expansion of violence and the collective character of hostilities;[98] the control of territory by non-State forces to the exclusion of government forces;[99] an increase in the number of government forces deployed to respond to the violence; the mobilization of volunteers and the type and distribution of weapons among the armed groups; the extent to which the local population has been displaced by the violence; and whether the situation has come to the attention of the Security Council.

Most commentators share the view that the high threshold of violence that is required for the existence of a non-international armed conflict means that it is unlikely that an armed conflict would be triggered by cyber means alone. Cyber-attacks like, for example, the alleged Trojan Horse attack on the security camera system in the Carmel Tunnels toll road in Israel on 8 September 2013 which caused hundreds of thousands of dollars in damage simply do not meet the requisite threshold of damage even if an organized armed group was to claim

---

[94] *Commentary on the Geneva Conventions of 12 August 1949* (ICRC 1952–1958) Vol. I 49.

[95] *Prosecutor v. Ljube Boškoski Johan Tarčulovski* (n 89) para 202.

[96] Ibid. para 198; *Prosecutor v. Ramush Haradinaj, Idriz Balaj, Lahi Brahimaj* (n 77) para 60.

[97] *Prosecutor v. Slobodan Milošević* (Trial Chamber Decision on Motion for Judgment of Acquittal) [2004] Case No. IT-02-54-T (Rule 98bis Decision) para 28.

[98] *Prosecutor v. Fatmir Limaj, Haradin Bala, Isak Musliu* (n 78) paras 94–134

[99] *Prosecutor v. Slobodan Milošević* (n 97) para 29.

responsibility for the attack.[100] The appropriate legal regime governing such conduct is the criminal law informed by international human rights law and not international humanitarian law. As Geiss has observed, not even the Stuxnet operation caused physical destruction of an intensity that approached the threshold of violence commonly required for a non-international armed conflict.[101]

It would however be short-sighted to categorically rule out the possibility that a cyber-attack by an organized armed group could trigger a non-international armed conflict. Consider, for example, a cyber-attack by an organized armed group on a civilian air traffic control system that resulted in effects of an equivalent magnitude to those perpetrated on 9/11. In such a case there seems to be little doubt that a State would consider itself to be engaged in a non-international armed conflict, without there having to be a series of comparable attacks.[102]

3. CONCLUDING COMMENTS

Only a decade ago the question of whether a cyber operation alone could trigger an international armed conflict in the absence of an existing conflict seemed more theoretical than a matter of pressing practical concern. However, with the increasing militarization of the cyber domain and the growing frequency and severity of hostile cyber operations directed at critical infrastructure – a trend that has escalated 'more rapidly than experts had anticipated' – the question is no longer simply academic.[103] Although some commentators were of the view that growing dependency on cyber infrastructure would likely lead to a downward adjustment of the threshold for an international armed conflict, the record so far indicates quite the opposite. States are displaying a significant level of circumspection even when confronted by serious and prolonged hostile cyber operations. One explanation for this 'resilience' is that States are simply not prepared to respond in kind until 'sufficiently certain'[104] of the identity of those responsible for the operation. False flag operations remain a real problem notwithstanding technological advances that are making attribution easier.[105] Paradoxically, if there is an upside to the problem of anonymity, it is the reticence by States to use force – cyber or kinetic – when confronted by hostile cyber operations.

Attribution aside, what is perhaps more problematic for conflict classification in the cyber age is that digital technologies have fundamentally disrupted our understanding of what constitutes power and violence. While the traditional view of power, epitomised by military superiority and the capacity to destroy adversaries is not entirely irrelevant, in a digital world power is about control, including through disorder, without necessarily resorting to kinetic force. If

---

[100] Daniel Estrin, 'AP Exclusive: Israeli Tunnel hit by cyber attack', *Associated Press* (27 October 2013) https://apnews.com/article/36f9d9b1b50d4faebf68dd84d052edc4.

[101] Robin Geiss, 'Cyber Warfare and Non-international Armed Conflicts' (2013) 89 *Intl L Studies* 627, 633.

[102] Most commentators have taken the view that a non-international armed conflict is unlikely to be triggered by a cyber-attack. See, e.g., Schmitt (n 15) at 258 and Droege (n 29) 551.

[103] ICRC Position Paper (n 5).

[104] Government of Netherlands (n 50).

[105] Kenneth Geers and others, 'World War C: Understanding nation-state motives behind today's advanced cyber attacks', *FireEye* (2013) https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf.

the primary concern of international humanitarian law is to limit violence and material harm – death, injury, damage and destruction – what role can it play or *should* it play in conflict that is concerned with control rather than the infliction of material violence?

Legal and policy developments have always been outpaced by advances in science and technology, not least in the context of war-fighting. Digital technologies are no exception. The attempt by States to redress this imbalance, demonstrated by the convening of the Open-Ended Working Group and re-convening of the Group of Governmental Experts in early December 2019, is a welcome step.[106] But until States are genuinely and fully committed to furthering peace rather than discord, to redirecting resources away from military expenditure toward the benefits that digital technologies have to offer, the instability that characterizes the cyber domain is likely to intensify for the foreseeable future.

[106] For further information, see https://www.un.org/disarmament/open-ended-working-group/ and https://www.un.org/disarmament/group-of-governmental-experts/.

20. Is the principle of distinction still relevant in cyberwarfare? From doctrinal discourse to States' practice

Karine Bannelier[1]

1. INTRODUCTION

A 'cardinal'[2] principle of humanitarian law, an 'intransgressible' principle of international customary law[3] – these are adjectives and superlatives which abound and celebrate the exceptional value of the principle of distinction in the law of war.

Initiated by the Lieber Code in 1863[4] and since then constantly reaffirmed, the principle of distinction, which is intended to protect civilians and civilian objects from 'the calamities of war'[5], was introduced in a general way in Article 48 of the First Additional Protocol to the Geneva Conventions of 1977. Article 48 provides that:

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.[6]

The principle of distinction has then manifested itself in several conventional as well as customary rules. The ICRC, for example, identified no less than 24 rules stemming from the principle of distinction in its 2005 study on customary international humanitarian law.[7]

[1] This work is supported by the French National Research Agency in the framework of the 'Investissements d'avenir' program (ANR-15-IDEX-02).

[2] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226, para 78.

[3] Ibid., para 79.

[4] Francis Lieber, *Instructions for the Government of Armies of the United States in the Field* (Government Printing Office 1898).

[5] Declaration Renouncing the Use, in Time of War, of Certain Explosive Projectiles (29 November/11 December 1868).

[6] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (8 June 1977) (Protocol I). As the ICRC opined, '[a]ccording to this principle, there is an obligation to distinguish at all times between civilians and civilian objects on the one hand, and military objectives on the other, and to take constant care in the conduct of military operations to spare the former'; ICRC, 'International humanitarian law and the challenges of contemporary armed conflicts', 32nd International Conference of the Red Cross and Red Crescent, 32IC/15/11 (Geneva, October 2015) 42, https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts.

[7] ICRC, 'I. The principle of distinction', *IHL Database, Customary IHL at* https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul.

This central principle to the law of armed conflict could not be ignored by the 2015 United Nations Group of Governmental Experts on Cybersecurity (UN GGE) landmark report. The Report 'notes the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction'.[8]

As the principle of distinction is self-evident, the Group limited itself to 'noting' it. No need to recognise or even affirm it, the syllogism is sufficient on its own: international law applies in cyberspace; distinction is an established international legal principle; distinction is applicable to cyberwarfare. Perhaps never in the history of war has a new technology been so easily accepted as being already 'covered' by existing law.

In *the Legality of the Use of Nuclear Weapons*[9] case, 25 years ago, some States tried to put forward an extreme version of voluntarism in relation to the application of existing law to nuclear weapons.[10] However, the International Court of Justice (ICJ) rejected such an interpretation of international law based on a very strict and probably incorrect reading of the old *Lotus* judgment. Recalling the fundamental principles of international humanitarian law,[11] including the Martens Clause according to which '[i]n cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience',[12] the Court stated that:

> [N]uclear weapons were invented after most of the principles and rules of humanitarian law applicable in armed conflict had already come into existence; (...). However, it cannot be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future.[13]

Like nuclear war, cyberwarfare is subject to the law of armed conflict and its 'cardinal principles', which are the prohibition on unnecessary suffering and the principle of distinction.[14] Limiting oneself to Articles 48, 51 and 52 of Protocol I and their customary rules, one could

---

[8] United Nations, General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Note by the Secretary-General, UN Doc A/70/174 (22 July 2015) para 28 (d).

[9] *Legality of the Threat or Use of Nuclear Weapons* (n 2).

[10] France, e.g., stated that, 'le principe selon lequel les limitations de souveraineté ne se présument pas a pour conséquence nécessaire qu'en l'absence de règles prohibant *expressément* le recours à la menace ou à l'emploi d'armes nucléaires en toute circonstance, ce recours doit être considéré comme *licite*, hors les circonstances particulières où il serait interdit'; ICJ Verbatim Record (1 November 1995) CR 95/23 63 (emphasis added). Russia added that, 'by virtue of the principle of sovereignty it is presumed that a State is free to act in absence of a specific restriction provided for in international law'; ICJ Verbatim Record (10 November 1995) CR 95/29 41.

[11] Especially art 22 of the Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907 (according to which '[t]he right of belligerents to adopt means of injuring the enemy is not unlimited', cited in *Legality of the Threat or Use of Nuclear Weapons* (n 2) para 77).

[12] Ibid., para 78. It is a reproduction of art 1(2) of Additional Protocol I (n 6).

[13] *Legality of The Threat or Use of Nuclear Weapons* (n 2) para 86.

[14] Ibid., para 78.

at least conclude that: first, cyber attacks directed against civilians and civilian objects are prohibited; second, civilian populations and individual civilians should enjoy protection against dangers arising from cyber military operations; and third, indiscriminate cyber attacks are prohibited.

These conclusions seem fairly reassuring when taking into account the potential significant effects of cyberwarfare on civilians. While cyber war is sometimes presented as less devastating than kinetic warfare due to the use of non-lethal and 'ultimate in precision weapons'[15] that weaken the enemy without necessarily destroying or killing,[16] cyber war nevertheless also raises fears of a devastating 'total war'.

As early as 2009, former US President Barack Obama expressed concern about what he described as a 'weapon of mass disruption'.[17] One year later, *The Economist* described in catastrophic terms a new form of warfare dominated by 'cyber-weapons': exploding oil refineries and pipelines, an out-of-control air traffic control system, derailed trains, lost financial data, a shut-down of power plants, among others. In short, an entire society ruined.[18]

The last few years and months have shown 'an evolution towards attacks disrupting the delivery of essential services to the population and attacks designed to cause physical effects'.[19] The Covid-19 epidemic is emblematic in this respect; there has been a major

---

[15] According to the US:

> [c]yber operations that result in non-kinetic or reversible effects can be an important tool in creating options that minimize unnecessary harm to civilians. In this regard, cyber capabilities may in some circumstances be preferable, as a matter of policy, to kinetic weapons because their effects may be reversible, and they may hold the potential to accomplish military goals without any destructive kinetic effect at all

United States Submission to the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2012–2013) 4. See also the US Law of War Manual according to which:

> In some cases, cyber operations that result in non-kinetic or reversible effects can offer options that help minimize unnecessary harm to civilians. In this regard, cyber capabilities may in some circumstances be preferable, as a matter of policy, to kinetic weapons because their effects may be reversible, and they may hold the potential to accomplish military goals without any destructive kinetic effect at all

United States of America, Office of General Counsel, Department of Defense, *Department of Defense Law of War Manual* (June 2015, updated December 2016) 1023. See also Jeffrey Kelsey, 'Hacking into international humanitarian law: The principle of distinction and neutrality in the age of cyber warfare' (2008) 106 *Michigan L Rev* 1434.

[16] As Glennon warned, 'cyber-operations can in this view be regarded as merely the latest efforts-the latest successes (...) to afford greater protection to non-combatant (and combatants), to enhance proportionality- in effect to pursue many of the ends of humanitarian law'; Michael J Glennon, 'The dark future of international cybersecurity regulation' (2013) 6 *J of National Security L & Policy* 569. See also Duncan Blake and Joseph S Imburgia, 'Bloodless weapons? The need to conduct legal reviews of certain capabilities and implications of defining them as 'weapons'' (2010) 66 *Air Force L Rev* 157.

[17] The White House, 'Remarks by the President on Securing our Nation's Cyber infrastructure' (Office of the Press Secretary, 29 May 2009) http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure, cited in Newton Lee, Counterterrorism and Cybersecurity (Springer 2013) 100.

[18] 'War in the Fifth Domain', *The Economist* (1 July 2010) http://www.economist.com/node/16478792.

[19] Laurent Gisel and Lukas Olejnik, 'The potential human cost of cyber operations: Starting conversation' (14 November 2018) I*CRC, The Humanitarian Law and Policy Blog*, https://blogs.icrc.org/law-and-policy/2018/11/14/potential-human-cost-cyber-operations/.

increase in cyber attacks that have targeted critical infrastructure and the health care sector.[20] In September 2020, for the very first time, a death was directly attributed to a cyber attack which targeted a hospital.[21] As opined by the ICRC:

> [O]n the one hand, cyber operations have the potential to enable parties to armed conflicts to achieve their military aims without harming civilians or causing physical damage to civilian infrastructure. On the other hand, recent cyber operations – which have been mostly conducted outside the context of armed conflict – show that sophisticated actors have developed the capability to disrupt the provisions of essential services to the civilian population.[22]

It is true that to date, beyond the Operation Glowing Symphony, the Russia-Georgia conflict of 2008 and the disruption of the Ukrainian power grid in 2015, most cyber operations suspected to have been sponsored by States have been conducted outside an armed conflict[23] and it has never been proven that their use during an armed conflict would have had harmful consequences on civilians, equivalent to the ones caused by the use of kinetic weapons.

However, '[t]he use of cyber operations during armed conflict is a reality'[24] since an increasing number of States have crossed the Rubicon and are developing cyber capabilities that they are ready to use. In this context, the 'potential cost'[25] of cyber operations for civilian populations and civilian objects raises growing concern about the capacity of the principle of distinction to provide a protective shield. Behind the reassuring words of the 2015 UN GGE, the application of the principle of distinction in cyberspace raises in fact important questions about its ability to curb the effects of this new form of war. It is true that some of these questions are not entirely new since the application of the principle of distinction has always been marked by more or less subjective and controversial interpretations;[26] but for several

---

[20] INTERPOL, 'INTERPOL repot shows alarming rate of cyberattacks during COVID-19' (4 August 2020) https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19. See also "Estonia's Statement at the Arria-formula meeting of the Security Council 'Cyber-Attacks Against Critical Infrastructure', Permanent Mission of Estonia to the UN (26 August 2020) https://un.mfa.ee/estonias-statement-at-the-arria-formula-meeting-of-the-security-council-cyber-attacks-against-critical-infrastructure/.

[21] Melissa Eddy and Nicole Perlroth, 'Cyber Attack Suspected in German Woman's Death', *The New York Times* (18 September 2020) https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.

[22] ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, ICRC position paper submitted to the 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' and the 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' (November 2019) 3, https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-icrc-on-initial-pre-draft-report-of-oewg.pdf.

[23] See the database of the Council for Foreign Relations, *Cyber-Operations tracker, on State-Sponsored Cyber Operations*, https://www.cfr.org/cyber-operations/.

[24] *International Humanitarian Law and Cyber Operations during Armed Conflicts* (n 22) 3, 'While only a few States have publicly acknowledged using such operation, an increasing number of States are developing military cyber capabilities, and their use is likely to increase in future'.

[25] ICRC, 'The Potential Human Cost of Cyber Operations', ICRC Expert Meeting, Geneva (14–16 November 2018) https://www.icrc.org/fr/publication/potential-human-cost-cyber-operations.

[26] As rightly observed by Dinniss, '[t]he principle of distinction has been under threat before'; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (CUP 2014) 182.

reasons cyber war stretches this debate to its limits.[27] Moreover, the failure of the UN GGE to adopt a report in 2017 explaining how international law applies in cyberspace was due, in part, to the reluctance of some States like Russia, China and Cuba to confirm the application of IHL or certain interpretations of IHL to cyber operations.[28] Recent debates within the UN OEWG[29] also create a great deal of uncertainty as to how the principle of distinction applies to cyberwarfare.

The objective of this chapter is to critically analyse the main debates concerning the application of the principle of distinction to cyberspace, based, whenever possible, on the practice of States and the views of the ICRC and experts.

At the heart of the debate is the question of whether the prohibition on direct attacks against civilians and civilian objects, which was adopted in the context of kinetic weapons, can fully apprehend the complexity of non-kinetic attacks whose effects are partially or completely dematerialised (Part 2). This question invites us to carefully re-read the principle of distinction in order to assess whether it is strictly focused on the prohibition of 'attacks' against civilians or whether it should also be interpreted as prohibiting military cyber operations below the threshold of an attack that directly target civilians (Part 3). Cyberwarfare also challenges the prohibition on indiscriminate attacks that stem from the principle of distinction. Indeed, the

---

[27] According to Dinniss, '[t]he additional targeting opportunities offered by computer network attack capabilities come at a time when there is already an increased tension in the laws of armed conflict over the continued pre-eminence of the principle of distinction in modern warfare'; ibid., 181.

[28] See e.g., the analysis of Michael N Schmitt and Liis Vihul, 'International cyber law politicized: The UN GGE's failure to advance cyber norms' (30 June 2017) *Just Security*, www.justsecurity.org/42768/ international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

[29] These three States have reiterated their criticisms before the UN OEWG and were joined by others States such as Iran. According to China:

> [w]e should be extremely cautious against any attempt to introduce use of force in any form into cyberspace, have sober assessment on possible conflicts and confrontations resulted from the indiscriminate application of the law of armed conflicts in cyberspace, and refrain from sending wrong messages to the world

China's Contribution to the Initial Pre-Draft of OEWG Report, https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf. In the same way, Russia declared that:

> [w]e regard as potentially dangerous the attempts to impose the principle of full and automatic applicability of IHL to the ICT environment in peacetime. This statement itself is illogical and contradictory, because IHL is applied only in the context of a military conflict while currently the ICTs do not fit the definition of a weapon

Commentary of the Russian Federation on the initial 'pre-draft' of the final report of the united nations open- ended working group on developments in the field of information and telecommunications in the context of international security, https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf; and Cuba considers that:

> [b]y acknowledging the applicability of IHL to the security dimension of ICTs, the international community would be recognizing the possibility of armed conflict in this field and therefore contributing to an increase in the present militarization of cyberspace. Furthermore, we consider that in a potential ICT related conflict there would be no need to protect combatants in the field, unless the State in question, was responding to an ICT attack with conventional weapons, thus legitimizing this misguided and unacceptable approach

Considerations on the initial pre-draft of the open-ended working group (OEWG) on developments in the field of information and telecommunications in the context of international security, https://front.un-arm.org/wp-content/uploads/2020/04/considerations-on-the-initial-pre-draft-of-the-oewg-cybersecurity-cuba-15-april.pdf.

nature and use of cyber tools combined with the interconnectivity of cyberspace make applying the principle of distinction all the more challenging (Part 4).

2. THE PROHIBITION OF CYBER ATTACKS AGAINST THE CIVILIAN POPULATION AND CIVILIAN OBJECTS

2(a) Could a Cyber Attack be an Attack under IHL? The Effects-based Approach

Not every cyber operation constitutes an attack in times of armed conflict. The main challenge concerning the application of the prohibition of cyber attacks against civilian populations and civilian objects lies in the definition of the attack itself. As Israel underlined recently, 'one of the key issues, in the conduct of hostilities in particular, is how to define "attacks" and in which circumstances cyber operations amount to attacks under LOAC'.[30] As the ICRC has also warned, 'the manner in which the notion of cyber "attack" is defined under the rules governing the conduct of hostilities (see Art 49 of Additional Protocol I) will greatly influence the protection that IHL affords to essential civilian infrastructure'.[31]

Firstly, it should be noted that the term 'attack' is particularly overused in the cyber domain, leading some commentators to remark that 'the definition of cyber-attack remains inconsistent'.[32] It is true that international law does not contain a unanimous definition of the term cyber attack and States have therefore proposed very broad definitions that go far beyond the notion of armed attack.[33] Even in the narrower sense of armed attack, the definition of cyber attack raises many questions and causes much controversy amongst States as to whether to apply the

---

[30] Roy Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (9 December 2020) EJIL: *Talk!*, https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/.

[31] International humanitarian law and the challenges of contemporary armed conflicts (n 6) 41, https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts.

[32] Jonathan A Ophardt, 'Cyber warfare and the crime of aggression: the need for individual accountability on tomorrow's battlefield' (2010) 9 *Duke L and Technology Rev* 1. See also 'Multinational Experiment 7 Outcome 3-Cyber Domain: Objective 3.3 - Concept Framework' (3 October 2012) 9, http://mne.oslo.mil.no:8080/Multinatio/MNE7produk/33CyberCon.

[33] According to Canada, e.g.:

> [c]yber-attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber-attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security;

Cyber Security Strategy of Canada (2010) 3, www.securitepublique.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-fra.pdf. For the UK:

> [t]he term cyber-attack can refer to anything from small-scale email scams through to sophisticated large-scale attacks with diverse political and economic motives. Large-scale attacks may have a number of interrelated aims such as: gaining unauthorized access to sensitive information; causing disruption to IT infrastructure; or causing physical disruption (e.g. to industrial systems)

quoted in NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/cyber-definitions.html.

jus ad bellum or *jus in bello* definition of attack. This controversy is largely fuelled by the fact that the conception of military cyber operations and attacks in the cyber domain is far removed from the traditional understanding of an 'armed attack' in the physical world. However, this has not prevented certain military manuals from adopting their own definition of a cyber attack. According to the *US Air Force Intelligence Targeting Guide* for example, 'computer network attacks are operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves'.[34] These cyber operations can take various forms, for example:

> gaining access to a computer system so as to acquire control over it, transmitting viruses to destroy or alter data, using logic bombs that sit idle in a system until triggered on the occasion of a particular occurrence or at a set time, inserting worms that reproduce themselves upon entry into a system and thereby overloading the network, and employing sniffers to monitor and/or seize data.[35]

Interesting and helpful as they may be, these definitions raise the question of how they correlate to the legal definition of 'attack' given by the law of war. Could the definition of 'attack' given by the law of war encompass cyber operations, and if so, which ones and based on what criteria?[36] The answer to this question is of fundamental importance for the effectiveness of the principle of distinction in cyberspace. Indeed, a definition of 'attack' strictly focused on the 'means' of the attack could exclude a wide range of cyber operations from the principle of distinction. Although applicable, the principle of distinction could therefore be of little use. However, this is not the case, as the identification of an attack under IHL is not based on the *means* of the attack but rather on its *consequences*.[37] Customary IHL defines 'attacks'

---

[34] 'US Air Force Intelligence Targeting Guide' (Air Force Pamphlet 14–210, 1 February 1998) http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.131.8965&rep=rep1&type=pdf. According to the lexicon of the Memorandum for Chiefs of the Military Services Commanders of the Combatant Commands, Directors of the Joint Staff Directorates:

> A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber-attack are not necessarily limited to the targeted computer systems or data themselves-for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber-attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber-attack may be widely separated temporally and geographically from the delivery

James E Cartwright, *Memorandum for Chiefs of the Military Services Commanders of the Combatant Commands, Directors of the Joint Staff Directorates* (2011) 5, http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

[35] Michael N Schmitt, 'Wired warfare: computer network attack and *jus in bello*' (2002) 84(846) *IRCC* 367.

[36] Oona A Hathaway and others, 'The law of cyber-attack' (2012) 100 *California L Rev* 817, 822–39.

[37] See, e.g., Heather Harrison Dinniss, 'Attacks and operations – The debate over computer network "attacks"', *New Technologies, Old Law: Applying International Humanitarian Law in a New Technological Age* (The Minerva Center for Human Rights, Jerusalem, 28–29 November 2011, Conference Paper 2) http://www.kas.de/israel/en/publications/29923/; Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) 415–6 (Rule 92 Definition of cyber-attack); Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (CUP 2004) 84.

as 'acts of violence against the adversary, whether in offence or in defence'[38] and, as Droege has shown, 'violence does not refer to the means of the attack – which would only encompass kinetic means. Military operations that result in violent consequences constitute attacks'.[39] This definition of violence makes it possible to qualify acts perpetrated by non-kinetic weapons as attacks when their effects are violent. As highlighted by Dörmann, 'the employment of biological or chemical agents that does not cause a physical explosion, such as the use of asphyxiating or poisonous gases, would constitute an attack' because the resulting effects are violent regardless of the means used to achieve them.[40] Like the use of chemical or biological agents, the use of cyber tools can constitute an attack. For example, according to the French paper on International Law Applied to Operations in Cyberspace, '[a]ny cyberoperation which is carried out in, and in connection with, an armed conflict situation, and constitutes an act of violence, whether offensive or defensive, against another party to the conflict, is an attack within the meaning of Article 49 of AP I to the Geneva Conventions'.[41]

2(b) Creeping from an Effects-based Approach towards a Kinetic Effects Equivalency Test?

A cyber operation is an attack under IHL when the consequences of the attack are violent. If there is consensus about this assumption, then what is the exact meaning of 'violent' and what is violence in cyberspace? Experts agree that, at the very least, an act that 'causes death or injury to persons or physical destruction or damage to objects' is an act of violence and could be qualified as an attack in cyberspace.[42] According to the Tallinn Manual, 'a cyber-attack is a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[43]

This 'effects-based approach' is merely analysed from the point of view of equivalence with kinetic effects. States that have made statements about the interpretation of the principle of distinction in cyberspace seem to agree at least that cyber operations that induce violent physical effects qualify as cyber attacks. For example, according to Australia, 'if a cyber operation rises to the same threshold as that of a kinetic "attack" (or act of violence) under IHL, the rules governing such attacks during armed conflict will apply to those kinds of cyber operations'.[44]

---

[38] Protocol I (n 6) art 49. This definition constitutes customary law. See, Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law* (vol I, Rules, ICRC, CUP 2006) 3–8.

[39] Cordula Droege, 'Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians' (2013) 94(886) *IRRC* 557.

[40] Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks', *CICR Resources* (19 November 2004) 4, https://www.icrc.org/eng/resources/documents/misc/68lg92.htm. See also *Prosecutor v Dusko Tadić* (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) [1995] No ICTY-94-1-A, para 1214.

[41] Ministère des Armées, *International Law Applied to Operations in the Cyberspace* (2019) 13, https://www.defense.gouv.fr/salle-de-presse/communiques/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international.

[42] Niels Melzer, *Cyberwarfare and International Law* (UNIDIR 2011) 26, http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

[43] Tallinn Manual 2.0 (n 37) 416–7 (Rule 92 Definition of Cyber-Attack).

[44] Australia's International Cyber Engagement, '2019 International Law Supplement, Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in

Likewise, the glossary of Denmark's Military Manual defines military computer network attacks as, 'network-based actions directed against IT networks, IT systems, or computers and expected to create an effect that may cause loss of human life, injury to persons, and/or substantial damage to or destruction of physical objects',[45] and according to the same manual, 'network-based operations must be regarded as attacks under IHL if the consequence is that they cause physical damage'.[46]

Examples of cyber operations that can therefore be considered attacks are numerous, as shown by the Tallinn Manual. For example, an intrusion into the computer control system of a nuclear power plant is not violent in itself, but it could be qualified as an 'attack' if its consequences are violent. One can also imagine a cyber operation that penetrates the central computer system of a chemical plant and that leads to the explosion of the installation and the release of toxic gases into the atmosphere. Here again, the intrusion is not violent, but its effects are violent: the explosion would cause damage to objects while toxic gases could have serious consequences on the health of the civilian population. This act could then be qualified as an attack.[47] The hacking of the computer control system of a dam could also be considered an 'attack' if it enables the hackers to take control of the dam and to open its valves causing massive flooding downstream. Here, the installation is not damaged, but the effects on civilians and infrastructure may be equivalent to a kinetic attack that would have destroyed the dam.[48]

Some States have also tried to put forward their own scenarios for cyber operations that could qualify as cyber attacks on the basis of the kinetic effect equivalency test. Denmark for instance has provided two examples of what it considers cyber attacks. One scenario refers to hacking 'into the adversary's *C4IS* system servers with a view to switching off the thermostatically controlled ventilation'.[49] According to Denmark, this constitutes an attack because it is 'injurious since the servers are physically damaged due to overheating'.[50] For Denmark, what constitutes an attack is also the '[h]acking into the software of a dam, which changes the programming so that potentially destructive waters could be released, or into the software of a waterworks so that drinking water and wastewater would be mixed'.[51]

To the extent that the victims are civilians, these attacks should be considered contrary to the principle of distinction. It is therefore clear that the kinetic effect equivalency test could be useful in terms of allowing the principle of distinction to cover a wide range of cyber operations and thus playing the protective role expected of it.

However, exclusively focusing on the physical effects in order to assess whether a cyber operation constitutes an 'attack' under IHL is also fraught with many difficulties; so much so

---

Cyberspace' (2019) https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html.

45 Danish Ministry of Defence, Defence Command Denmark, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations* (September 2016) 677.

46 Ibid., 291.

47 Tallinn Manual 2.0 (n 37) 415–6 (Rule 92 Definition of Cyber-Attack).

48 Ibid.

49 C4IS: Command, Control, Communications, Computers and Information System.

50 Danish Ministry of Defence (n 45) 291.

51 Ibid.

that one might even wonder whether relying exclusively on the '[k]inetic effect equivalency test' in this field might jeopardise the principle of distinction.[52]

Indeed, one might wonder whether a strict and/or exclusive application of the 'kinetic effect equivalency test' would authorise and legitimise a wide range of military operations against civilians that would never have been considered acceptable if they had been carried out by kinetic force.

2(c) A Controversial Creeping Effect? The Limits of the Kinetic Effect Equivalency Test

The 'kinetic effect equivalency test' assumes that damage can be clearly identified. But this assumption raises certain questions. First, proof of the existence of damage caused by cyber operations, and the precise extent of this damage, could become a real *probatio diabolica*, especially if one takes into consideration that the effects of cyber attacks could be, unlike the effects of kinetic weapons, somewhat indirect (see section 2(c)(i)). The 'kinetic effect equivalency test' in fact raises the fundamental question of whether the damage even *exists* when it is not strictly physical (see section 2(c)(ii)) and raises a further question as to what constitutes an object in cyberspace and whether intangible things, like data, could be protected as 'objects' by IHL (see section 2(c)(iii)).

2(c)(i) Assessing damages resulting from cyber operations: the problem of indirect or reverberating effects

In applying the effects test, it is important to assess not only the consequences of a cyber operation against civilian infrastructures but also the effects of these effects on individuals. This is why the ICRC and some countries like France have underlined the need to include the 'indirect' and/or 'reverberating' effects of an attack in the assessment.

However, the causal proximity between the impairment of the functioning of a system and any indirect damage to the civilian population is often difficult to establish with certainty and can sometimes lead to a dead end.[53] To avoid this impasse, it is often asserted that it is the 'reasonable, foreseeable' effects that must be assessed, rather than the actual effect itself.

According to the ICRC, 'all operations expected to cause death, injury or physical damage constitute attacks, including when such harm is due to foreseeable indirect or reverberating effects of an attack, such as the death of patients in intensive-care units caused by a cyberattack against the electricity network that then cuts the hospital electricity supply'.[54] For France:

---

[52] See, e.g., the analysis of Elizabeth Mavropoulou, 'Targeting in the cyber domain: Legal challenges arising from the application of the principle of distinction to cyber attacks' (Spring 2015) 4 *Journal of Law & Cyber Warfare* 23, 32–6.

[53] In 2003, after the blackout occurred on the east coast of the US, 11 direct victims related to this event were counted. Most of them were victims of accidents caused by malfunctioning of electrical equipment: vehicle collisions due to the cessation of traffic lights, asphyxia caused by damaged electrical generators, etc. The indirect effects of the blackout and their consequences in the mid and long term do not seem to have been evaluated. Indeed, it is difficult, if not impossible, to determine, e.g., how many people with serious illnesses could not receive treatment or how many surgeries were postponed, and what were the implications of these adjournments and postponements on the health of the patients.

[54] International humanitarian law and the challenges of contemporary armed conflicts (n 6) 41, https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts.

> [t]he assessment of the effects of a cyberoperation takes into account all the foreseeable damage caused by the cyber weapon, whether direct (such as damage to the ICT equipment directly targeted or interruption of the system) or indirect (such as the effects on the infrastructure controlled by the targeted system, or on persons affected by the malfunction or destruction of the targeted systems or infrastructure, or by the alteration and corruption of content data).[55]

The Tallinn Manual also recognises that the prohibition of attacks 'is not limited to effects on the targeted system. Rather, it encompasses any reasonably foreseeable consequential damage, destruction, injury or death'.[56]

The use of such an 'indeterminate terminology' to qualify a cyber operation as an attack can give rise to even more questions.

It is true that 'key principles of IHL require parties to armed conflict to anticipate the effects of attack'[57] as this is notably the case in relation to the application of the principle of distinction and the protection of the civilian population. For example, Article 51 of Protocol I qualifies as an indiscriminate attack one 'which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated'. However, as is often the case with the 'infinitely obscurantist possibilities of legal language and the wonderous opacities of legal syntax',[58] this kind of 'normative indeterminacy' gives belligerents a large margin of appreciation. Taking into account the fact that in the physical world the assessment of the effects of an operation often lead to controversy despite the fact that their consequences 'are generally straightforward to anticipate',[59] one may wonder what can be 'reasonably foreseeable' in the cyber domain.

According to the ICRC, 'uncertainty about the effects of an operation [is] an inherent feature of cyber operations'[60] while 'actual effects of a malware became apparent only once it was released'.[61] Moreover, as underlined by two experts:

> At a practical level, the outcomes of cyber operations can be much more uncertain than physical operations, and evidence of whether any damage has occurred at all may be unavailable. This is so for a number of reasons. Harms that originate in code may be latent or transient. They may rely on the confluence of a number of different events to achieve their peak damage. Failures in technical systems may emerge for reasons that have nothing to do with code that is deliberately introduced. And victim States may have incentive to keep secret the harm they have suffered so as not to project an image of vulnerability to the broader community.[62]

---

55 Ministère des Armées (n 41) 16.

56 Tallinn Manual 2.0 (n 37) 416.

57 ICRC, 'The Potential Human Cost of Cyber Operations', ICRC Expert Meeting, Geneva (14-16 November 2018) 38, https://www.icrc.org/fr/publication/potential-human-cost-cyber-operations.

58 W Michael Reisman, 'International politics and international law-making: reflections on the so-called "politization" of the International Court' in Wybo Heere (ed), *International Law and its Sources-Liber Amicorum Maartens Bos* (Kluwer 1988) 88.

59 Sasha Romanosky and Zachary Goldman, 'Understanding cyber collateral damage' (2017) 9 *Journal of National Security Law and Policy* 233, 237.

60 ICRC, 'The Potential Human Cost of Cyber Operations', ICRC Expert Meeting, Geneva (14-16 November 2018) 38, https://www.icrc.org/fr/publication/potential-human-cost-cyber-operations.

61 Ibid. 39.

62 Romanosky and Goldman (n 59).

While more and more States are developing military cyber capabilities and seem ready to use them, one wonders how many of them have developed an adapted methodology for estimating damages and casualties of cyber operations. Only a few States, such as Australia, the US, France and Spain, have publicly declared that they are applying such a methodology.[63] However, to date it remains unsettled whether this methodology is accurate enough to assess what is 'reasonably foreseeable'. As for the others, the question is whether they even seek to assess the effects of their cyber operations.

Moreover, the seriousness of injuries resulting from a cyber operation varies and depends on different parameters, such as the dependence of a society on certain systems, their resilience and the appropriateness of human responses to these events.[64] As illustrated by cyber operations conducted against Estonia in 2007 and Georgia in 2008, a wired society such as Estonia may be more vulnerable[65] than a 'less computer relevant' society such as Georgia.[66] It is also possible that less connected countries may be more heavily dependent on certain facilities and infrastructure. Additionally, variations in the nature of the operation can lead to significantly different results as evidenced by military operations against electrical grids in Iraq in 1991 and in Serbia and Montenegro in 1999.[67]

---

[63] France, e.g., considers that:

> [i]n order to ensure application of the rules governing the conduct of hostilities (distinction, proportionality and precaution, prohibition of superfluous injury and unnecessary suffering), a specific digital targeting process is used for cyberoperations, under the responsibility of the commander-in-chief of the armed forces, with the input, inter alia, of operational staff and specialist operational legal advisers

Ministère des Armées (n 41) 14; in the US, the USCYBERCOM has adopted in 2016 a document which is entitled 'Improving Targeting Support to Cyber Operation'; in the same way Spain published in 2019 a *Doctrina De Targeting Conjunto*, which seems to fully include the cyber dimension (Estado Mayor de la Defensa, *Doctrina De Targeting Conjunto,* 2019, https://www.defensa.gob.es/ceseden/Galerias/ccdc/documentos/PDC_3_9_xAx_Doctrina_Targeting_Conjunto.pdf); and Australia affirms that:

> All Australian military capabilities are employed in line with approved targeting procedures. Cyber operations are no different. Australian targeting procedures comply with the requirements of IHL and trained legal officers provide decision- makers with advice to ensure that Australia satisfies its obligations under international law and its domestic legal requirements

(Australia's International Cyber Engagement, 'Annex A: Australia's position on how international law applies to state conduct in cyberspace', https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/annexes.html).

[64] David Turns, 'Cyberwarfare and the notion of direct participation in hostilities' (2012) 17 *J of Conflict and Security L* 279, 288.

[65] As underlined in a Report published in 2010 about Estonia, *International Cyber Incidents: Legal Considerations*:

> The high availability of public e-services and wide Internet accessibility that the Estonian population enjoys have, as a negative side effect, also made the country a more attractive target for cyber-attacks. The dependency of the population on easily accessible online services has made the society more vulnerable to large scale disruptions in the availability of Internet access

Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations* (NATO CCDCOE 2010) 18.

[66] Turns (n 64) 287.

[67] In a 2003 Report, Human Rights Watch underlined that:

> Attacks on electrical generation facilities used by the civilian population would have a profound and long-term impact on the civilian population in Iraq. During the 1991 Persian Gulf War, for example, the failure of American war planners to accurately assess the cascading effects that

Last but not least, one should take into account that the assessment of damage resulting from cyber operations is even more difficult and controversial due to the fact that such damage may have long-term effects.[68] This raises the question of when such an 'attack' should be assessed as having taken place. Is it reasonable to retrospectively label an act as an attack days, weeks or even months after its commission?

Therefore, depending on the circumstances and on a series of hardly identifiable parameters, the same act could or could not be qualified as an attack. Paradoxically, this could lead to an absurd syllogism in that a resilient civilian infrastructure which is not subject to attacks as defined above could then easily become the target of more cyber operations.

These questions are, however, not new. They are the kind of questions that are also raised in relation to kinetic operations when assessing the proportionality of an attack or the indiscriminate nature of an attack. But while a kinetic attack against an installation will necessarily cause direct physical damage, this is not automatically the case where a cyber operation is concerned.

Indeed, a cyber operation against a facility can be more insidious in the sense that it can generate collateral damage without causing *direct* damage to the targeted installation. Even worse, a cyber attack could be conducted against an installation in a completely concealed and secretive way.

In his Cold War memoirs, former Air Force Secretary Thomas Reed recalls how, in 1982, a US satellite detected a large blast in Siberia. It was, according to him, 'the most monumental non-nuclear explosion and fire ever seen from space'. This blast, he said, 'was a malfunction in the computer-control system that Soviet spies had stolen from a firm in Canada. They did not know that the CIA had tampered with the software so that it would "go haywire", after a decent interval'.[69]

Even today, numerous viruses and worms remain undetectable in many countries. It would then not be a big surprise to them that a malfunction at a facility is the result of a cyber attack.

2(c)(ii) Beyond physical damage? Loss of functionality without physical damage and destruction v. neutralisation

Cyber war profoundly modifies the parameters of war. As Dinniss has explained:

> attacks on electricity would have on the civilian population had profound humanitarian consequences. These attacks crippled basic civilian services, including hospital-based medical care, and shut down water-distribution, water-purification, and sewage-treatment plants. As a result, the most vulnerable members of the population, young children and adults requiring medical attention, suffered injury and death from the lack of potable water and poor medical treatment. It was proven in Yugoslavia that attacks on electrical distribution facilities can achieve the necessary military effect of disrupting power supply without long-term incapacitation of electrical generation capability. Due to the severe consequences that followed destruction of electrical generation in Iraq, the US attacked similar facilities in Kosovo in such a way as to cause only temporary incapacitation.

Human Rights Watch, 'International humanitarian law issues in a potential war in Iraq' (Human Rights Watch Briefing Paper 2003) 8–9 http://www.hrw.org/sites/default/files/reports/Iraq%20IHL%20formatted.pdf.

[68] Thomas W Smith, 'The new law of war: Legitimizing hi-tech and infrastructural violence' (2002) 46 *Intl Studies Quarterly* 363.

[69] Thomas Reed, *At the Abyss: An Insider's History of the Cold War* (Presidio Press/Ballantine Books 2004) 368.

> Computer network attacks not only increase the number of targets that it is possible to attack by reducing the collateral damage and hence the proportionality equation in target selection, they also allow the possibility of operations which cause no physical damage but nonetheless destroy or merely neutralize the object or system in question. This is an attractive option for states, particularly in conflicts which will necessitate the reconstruction of the battle-space at the conclusion of hostilities; it is inefficient to bomb a power generating station if you can simply turn it off.[70]

What needs to be assessed then is how to characterise the cyber operations 'that do not have a clear kinetic parallel'.[71] Are they excluded from the notion of attack or do we determine that the mere neutralisation of an installation or interference with its normal operation, or the loss of functionality qualifies as an 'attack'?[72] Here again the practice is scarce and sometimes ambiguous as it is illustrated by the position of New Zealand according to which: 'A cyber activity may constitute an "attack" for the purposes of international humanitarian law where it results in death, injury, or physical damage, *including loss of functionality*, equivalent to that caused by a kinetic attack.[73]

There is therefore a real risk that a narrow definition of attack which is limited to the assessment of physical damage could rob the principle of distinction of its main effects. As the ICRC has warned:

> If the notion of attack is interpreted as only referring to operations that cause death, injury or physical damage, a cyber operation that is directed at making a civilian network (such as electricity, banking, or communication) dysfunctional, or is expected to cause such effect incidentally, might not be covered by essential IHL rules protecting the civilian population and civilian objects.[74]

Despite this warning, some States and experts seem to be applying the kinetic effect equivalency test in a strict and exclusive manner. For example, Israel considers that 'an act will constitute an attack only if it is expected to cause death or injury to persons or physical damage to objects, beyond de minimis'.[75] Relying on commentaries of Protocol I stressing that violence requires the use of physical force,[76] the Tallinn Manual also states that '[i]nterference with functionality qualifies as damage if restoration of functionality requires replacement of physical components'.[77] A cyber operation that results in the suspension of normal activity of

---

[70] Dinniss (n 26) 183–4.

[71] Harold Koh (Legal Advisor, US Department of State) opined: 'As you all know, however, there are other types of cyber actions that do not have a clear kinetic parallel, which raise profound questions about exactly what we mean by "force"': Harold H Koh, *International Law in Cyberspace* (U.S. Department of State, 18 September 2012) http://www.state.gov/s/l/releases/remarks/197924.htm.

[72] See Gary D Brown, 'International law applies to cyber warfare! Now what?' (2017) 46 *Southwestern Law Review* 355, 369–71.

[73] New-Zealand Foreign Affairs and Trade, *The Application of International Law to State Activity in Cyberspace* (1 December 2020) para 26, (emphasis by the author), https://www.mfat.govt.nz/en/media-and-resources/ministry-statements-and-speeches/cyber-il/#:~:text=Brexit,The%20Application%20of%20International%20Law%20to%20State%20Activity,01%20Dec%202020&text=1.,responsible%20state%20behaviour%20in%20cyberspace.

[74] *International Humanitarian Law and Cyber Operations during Armed Conflicts* (n 22) 8.

[75] Schöndorf (n 30).

[76] Michael Bothe, Karl Josef Partsch and Waldemar A Solf, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (Martinus Nijhoff 1982) 289.

[77] Tallinn Manual 2.0 (n 37) 417.

a plant does not constitute an attack as such, unless the resumption of operation of the system requires the physical replacement or reinstallation of certain components, or collateral damage that has been produced due to the malfunction of the system, which meets the kinetic effect equivalency test requirements. Moreover, the damage should be physical.[78] As a consequence, cyber operations that cause mere 'inconvenience' do not qualify as an attack.[79]

However, this interpretation is controversial for various reasons and, contrary to the Tallinn Manual, it seems difficult, for the time being, to deduce the existence of a customary rule that excludes non-physical damage.

First, it should be underlined that, as the ICRC stated, 'there is no definition of "inconvenience" and "this terminology is not used in IHL"'.[80] It therefore seems troublesome to use non-existent terminology to determine the scope of a legal obligation. Moreover, States do not have enough experience with regard to this issue and the few statements dedicated to it show only this: that States are divided. France, for instance, is perhaps the only country to date that has addressed this problem directly and openly. It considers that:

> [c]ontrary to the definition given by the Tallinn Manual Group of Experts, France does not characterize a cyberattack solely on the basis of material criteria. It considers that a cyberoperation is an attack where the targeted equipment or systems no longer provide the service for which they were implemented, whether temporarily or permanently, reversibly or not. If the effects are temporary and/or reversible, the attack is characterized where action by the adversary is necessary to restore the infrastructure or system (repair of equipment, replacement of a part, reinstallation of a network, etc.).[81]

The conclusion is clear: 'Contrary to the Tallinn Manual, France considers that an attack within the meaning of Article 49 of AP I may occur even if there is no human injury or loss of life, or physical damage to goods'.[82] This view is supported by certain commentators.[83]

It can also be aid that the existence of physical damage is not a *sine qua non* requirement for a cyber operation to qualify as an attack to the extent that a mere 'neutralization' can, in certain circumstances, qualify as an attack.[84] This interpretation is supported by IHL rules. As Dörmann states:

> Given that elsewhere in the same section of AP I [Additional Protocol I], namely in the definition of a military objective, reference is made to *neutralization* of an object as a possible result of an attack,

---

[78] According to Schmitt, 'a cyber operation, like any other operation, is an attack when resulting in death or injury of individuals, whether civilians or combatants, or damage to or destruction of objects, whether military objectives or civilian objects'; Michael N Schmitt, 'Cyber operations and the jus in bello: Key issues' (2011) 87 *Naval War College Intl L Studies* 89, 94.

[79] Tallinn Manual 2.0 (n 37) 418.

[80] International humanitarian law and the challenges of contemporary armed conflicts (n 6) 42.

[81] Ministère des Armées (n 41) 13.

[82] Ibid.

[83] Droege (n 39) 557–61.

[84] According to France:
> the destruction of adversary military offensive cyber or conventional capabilities by disruption or the creation of major damage is an attack within the meaning of IHL. The same applies to neutralisation actions which damage adversary cyber or conventional military capabilities by destroying ICT equipment or systems or altering or deleting digital data or flows such as to disable a service essential to the operation of such capabilities.

Ministère des Armées (n 41) 13.

> one may conclude that the mere disabling of an object, such as shutting down of the electricity grid, without destroying it should be qualified as an attack as well.[85]

Likewise, Droege has noted that the term 'neutralization' in Article 52(2) of Protocol I:

> shows that that the drafters had in mind not only attacks that are aimed at destroying or damaging objects, but also attacks for the purpose of denying the use of an object to the enemy without necessarily destroying it. So, for instance, an enemy's air defence system could be neutralized through a cyber-operation for a certain duration by interfering with its computer system but without necessarily destroying or damaging its physical infrastructure.[86]

Whatever the arguments put forward by each camp in support of their claims, this controversy shows that the assimilation of cyber war into conventional warfare induced by the 'kinetic effect equivalency test' is not always an easy task and may even be perceived as a reductive one. Faced with the dematerialization of the initial act, it seems that its effects are 're-materialized' in order to grasp this phenomenon. But attempting by all means to make cyber war fit the classical framework risks excluding a wide range of military cyber operations that are directed against civilians and civilian objects. As Schmitt has opined:

> if the Serbian State television station had been targeted by CNA rather than kinetic weapons during NATO strikes on Belgrade in April 1999, there might well have been no consequent injury, death, damage or destruction. In that circumstance, criticism on the basis that a civilian target had been hit would probably have fallen on deaf ears and thereby avoided the resulting negative publicity, as well as the resulting litigation in the European Court of Human Rights.[87]

But if this assertion is true it could lead us, as Droege has warned, to the absurd conclusion 'that the destruction of one house by bombing would be an attack, but the disruption of an electrical grid supplying thousands or millions of people would not'.[88]

Finally, it seems that according to Kelsey '[t]he potentially non-lethal nature of cyber weapons may cloud the assessment of an attack's legality, leading to more frequent violations of the principle of distinction in this new form of warfare than in conventional warfare'.[89]

---

[85] Dörmann (n 40) 4, https://www.icrc.org/eng/resources/documents/misc/68lg92.htm.

[86] Droege (n 39) 558.

[87] Michael N Schmitt, 'Wired warfare: computer network attack and *jus in bello'* (2002) 84 *IRRC* 381.

[88] Droege (n 39) 558–9.

[89] Jeffrey Kelsey, 'Hacking into international humanitarian law: The principle of distinction and neutrality in the age of cyber warfare' (2008) 106 *Michigan L Rev* 1430, 1439. As Schmitt has also pointed out:

> many cyber operations that might be directed at civilian infrastructure or otherwise have serious adverse consequences for the civilian population would arguably not qualify as cyber-attacks, and would accordingly lie beyond the reach of IHL's rules on attack … [U]ncertainty with respect to the loss of functionality threshold leaves the legal characterization of certain cyber operations directed at or affecting the civilian population ambiguous. A party to the conflict could exploit such uncertainty to avoid consensus condemnation as unlawful of cyber operations that are directed at or otherwise affect civilian cyber infrastructure. From a humanitarian perspective, this situation is untenable

Michael N Schmitt, 'Wired warfare 3.0: Protecting the civilian population during cyber operations' (2019) 101 *IRRC* 333, 340.

2(c)(iii) From physical to intangible objects and the data battlefield

For the ICRC, operations that imperil essential civilian data 'could cause more harm to civilians than the destruction of physical objects'.[90] It is true that data are everywhere today; they are an essential part of our lives, and they are also essential for the development of Artificial Intelligence. It is therefore not surprising that data are becoming a prime target for belligerents.[91] The data battlefield is here to stay for good. It is therefore crucial to assess to what extent operations that imperil data could qualify as an attack. In this respect the main issue is whether or not data is an object.[92] According to the ICRC, 'the question of whether and to what extent civilian data constitute civilian objects remains unresolved'.[93] Declarations by States on this question are indeed scarce and the doctrine is not united.[94]

First, it is worth noting that according to certain interpretations 'data are not regarded as "objects" under IHL'.[95] According to Israel, 'only tangible things can constitute objects' and only objects are protected by the principle of distinction. For Israel, the principle of distinction is 'object dependent'.[96] Here again, the reasoning appears to be clear: data are not physical; thus, they are not objects; not being objects there is no attack; with no attack there is no principle of distinction. The only way to integrate data into the principle of distinction is to prove that the 'deletion or alteration' of data is 'reasonably expected to cause physical damage to objects or persons and fulfills the other elements required to constitute an attack'.[97] And the Tallinn Manual seems to follow the same reasoning by saying that targeting essential civilian infrastructure does not constitute an attack as long as it does not cause physical damage.[98]

On the other hand, for others, data are protected by the principle of distinction in the same way as objects. According to France, '[a]lthough intangible (…) civilian content data may be deemed protected objects, contrary to the position of the majority of the Tallinn Manual Group of Experts. The special protection afforded to certain objects extends to systems and the data that enable them to operate'.[99] And, as a consequence, '[g]iven the current state of digital dependence, content data (such as civilian, bank or medical data, etc.) are protected under the principle of distinction'.[100] Less firmly perhaps, but still interestingly, Finland also considers that:

---

90 *International Humanitarian Law and Cyber Operations during Armed Conflicts* (n 22) 8.

91 According to France, for instance, '[i]n an armed conflict situation, the primary purpose of cyber weapons is to produce effects against an adversary system in order to alter the availability, integrity or confidentiality of data'; Ministère des Armées (n 41) 13.

92 Schmitt (n 89) 340–3.

93 *International Humanitarian Law and Cyber Operations during Armed Conflicts* (n 22) 8.

94 For a detailed analysis of the doctrine see Kubo Mačák, 'This is Cyber: 1 + 3 Challenges for the Application of International Humanitarian Law in Cyberspace', Exeter Centre for International Law (Working Paper Series 2019/2) 9–11; Kubo Mačák, 'Military Objectives 2.0: The case for interpreting computer data as objects under international humanitarian law' (2015) 48 *Israel Law Review* 55, for whom 'the concept of military objectives in IHL should properly be construed to include computer data'. See also for a synthesis Tim McCormak, 'International Humanitarian Law and the targeting of Data' (2018) 94 *Int'l L. Stud* 222.

95 Danish Ministry of Defence (n 45) 310.

96 Schöndorf (n 30) 6.

97 Ibid.

98 Tallinn Manual 2.0 (n 37) 416 (Rule 92 Definition of Cyber-Attack).

99 Ministère des Armées (n 41) 15.

100 Ibid.

> cyber means and methods of warfare must be used consistently with the principles of distinction, proportionality and precautions, as well as the specific rules flowing from these principles. (…) Constant care shall be taken to ensure the protection of civilians and civilian objects, including essential civilian infrastructure, civilian services and civilian data.[101]

In fact, the question is whether to read the principle of distinction 'avec des lunettes de notaire' (with 'notary glasses') or from the perspective of its purpose. As warned by the ICRC:

> the assertion that deleting or tampering with such essential data would not be prohibited by IHL in today's data-reliant world seems difficult to reconcile with the object and purpose of IHL (…). Excluding essential civilian data from the protection afforded by IHL to civilian objects would result in an important protection gap.[102]

In the absence of an understanding amongst States about this issue, it is useful to examine to what extent the principle of distinction could be interpreted as prohibiting not only cyber attacks but also cyber operations.

3. NO ATTACK, NO DISTINCTION? BEYOND THE CONCEPT OF ATTACK: PROHIBITION OF MILITARY CYBER OPERATIONS DIRECTED AGAINST CIVILIANS?

The debate about how to apply the principle of distinction to military operations that are directed against civilians but are below the threshold of an attack is not a new one, but it was probably less pertinent when applied to the traditional use of kinetic weapons than it is today when applied to cyber operations. Given the controversies surrounding the interpretation of the notion of 'attack' in cyberspace, one wonders whether and to what extent the principle of distinction could be applied to operations for which their qualification as 'attacks' remains controversial. The cyber world is heralding a new battle arena of seemingly infinite size, in which the core of civilian society is the target. Applying the principle of distinction to hostile cyber operations (even if they do not qualify as 'attacks') that are exclusively targeting civilians, maybe, the best way to preserve the *raison d'être* of the principle of distinction and its full relevance to cyberwarfare.

However, the question remains for the time being largely unanswered. Even the ICRC seems hesitant on this issue. Despite the fact that in 2015 the ICRC seemed to be clearly in favour of applying the principle of distinction to cyber operations below the level of an attack by opining that even cyber operations that would constitute 'military operations' without amounting to 'attacks' *per se* are governed by the principle of distinction,[103] in 2019 its position as expressed in the OEWG seemed to have become more nuanced. As it said: 'most rules stemming from the principles of distinction, proportionality and precautions – which provide

---

[101] Finland, Ministry of Foreign Affairs, *International law and cyberspace Finland's national positions* (2020) 7 https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859.

[102] *International Humanitarian Law and Cyber Operations during Armed Conflicts* (n 22) 8.

[103] International humanitarian law and the challenges of contemporary armed conflicts (n 6) 42.

general protection for civilians and civilian objects – apply *only* to military operations that qualify as "attacks" as defined in IHL'.[104]

It is true that the ICRC is not saying here that the principle of distinction does not apply to cyber operations in general but that 'most rules stemming' from the principle of distinction apply only to attacks. 'Most' does not mean 'all' but the ICRC does not provide any more information about these rules, thereby raising more questions and uncertainties than answers. This hesitation from the ICRC illustrates well the division between States and experts on this question.

As for the Tallinn Manual, the answer is clear: military operations against civilians are prohibited by the principle of distinction *only to the extent* that these operations meet the threshold of an attack.[105] This interpretation is clearly shared by at least one State, Israel, which considers that 'only acts amounting to attacks are subject to the "targeting rules" relating to distinction, precautions and proportionality'.[106] As explained by Schmitt, 'cyber operations directed against civilian computer systems do not violate the prohibition on attacking civilian objects unless they qualify as an attack by virtue of their consequences'.[107] According to this interpretation, belligerents have the right to target civilians and civilian objects as long as no direct physical damage occurs,[108] or, at least, no 'reasonably foreseeable' damage. As a result, cyber operations that imperil, for instance, essential civilian data should not be covered by the principle of distinction.

Beyond Israel's clear statement on this issue, it is difficult to determine what other States think. In contrast to Israel, Australia stated that:

> [a]pplicable IHL rules will also apply to cyber operations in an armed conflict that do not constitute or rise to the level of an 'attack', including the principle of military necessity and the general protections afforded to the civilian population and individual civilians with respect to military operations.[109]

If State practice is still too scarce to reach a definitive conclusion on this issue, it should however be noted that several elements could advocate in favour of an application of the prin-

---

[104] Ibid., 7 (emphasis by the author).

[105] According to the Tallinn Manual, '[o]nly when a cyber-operation against civilians or civilian objects (or other protected persons and objects) rises to the level of an attack is it prohibited by the principle of distinction and those rules of the law of armed conflict that derive from the principle'; Tallinn Manual 2.0 (n 37) 422.

[106] Schöndorf (n 30) 5.

[107] Michael N Schmitt, 'International law in cyberspace: The Koh Speech and Tallinn Manual juxtaposed' (2012) 54 *Harvard Intl L J* 26. See also Schmitt (n 78) 91.

[108] According to Davidson:

> non-military objectives can be targeted by CNAs, as long as the result is not physical danger to the civilian population or damage to civilian objects and the intention of such action is not to terrorize the civilian population. This is so, even if the motive of the operation is military and it is conducted by armed forces'; Osnat Davidson, 'A legal analysis of computer network attacks under international law

(2007–2008) 3 *IDF L Rev* 70, 92.

[109] Australia's International Cyber Engagement, '2019 International Law Supplement, Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace', https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html.

ciple of distinction to hostile military cyber operations against civilians below the threshold of attack.

A grammatical reading of the articles that codify the principle of distinction could lead us to conclude that military cyber operations against civilians should be considered as being prohibited. Article 51 of Additional Protocol I for instance states that '[t]he civilian population and individual civilians shall enjoy general protection against dangers arising from military *operations*'; Article 48 asks belligerents to 'direct their *operation*s only against military objectives'; and Article 57 adds that 'In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects'.[110] The combination of these articles goes beyond the notion of attack and has led some experts to conclude that:

> [A]lthough attacks certainly represent the predominant form of combat operation, it would be inaccurate to assume that not amounting to an attack are not subject to IHL governing the conduct of hostilities. Accurately understood, the applicability of the restraints imposed by IHL on the conduct of hostilities to cyber operations depends not on whether the operations in question qualify as 'attacks' (that is, the predominant form of conducting hostilities), but on whether they constitute part of the 'hostilities' within the meaning of IHL.[111]

Taking into consideration how warfare can develop dramatically in the digital world, it would be unreasonable and perhaps counterproductive to 'stick' to a fixed and inflexible interpretation of the conditions of the principle of distinction. On the contrary, the law of armed conflict should, perhaps, be interpreted in an evolutive way in order to adapt to the new reality of war and the new capacities to wage war. International courts and treaty bodies, faced with changes in technology and science, have often used dynamic and evolutive interpretation of international treaties as well as principles of international law to give them their full effect.[112]

For example, it is due to such a dynamic interpretation by judges that the principle of due diligence came out of the Strait of Corfu to irrigate almost all fields of international law.[113]

In 1997 in its *Gabčikovo-Nagymaros* judgment, the ICJ held that the bilateral agreement concluded in 1977 between Czechoslovakia and Hungary should be interpreted, not according to the law and scientific knowledge as they existed in 1977, but dynamically aligned with

---

[110] According to Melzer:

> [t]he basic treaty rule of distinction is not formulated in terms of 'attack' but in terms of 'operations' (...). Therefore, although attacks certainly represent the predominant form of combat operation, it would be inaccurate to assume that cyber operations not amounting to an attack are not subject to IHL governing the conduct of hostilities. Accurately understood, the applicability of the restraints imposed by IHL on the conduct of hostilities o cyber operations depends not on whether the operations in question qualify as 'attack' (that is, the predominant form of conducting hostilities), but on whether they constitute part of the 'hostilities' within the meaning of IHL

Melzer (n 42) 27. See also Dinniss (n 37).

[111] Melzer (n 42) 27.

[112] See Giovani Distefano, 'L'interprétation évolutive de la norme internationale' (2011) 112 *RGDIP* 373; Rosalyn Higgins, 'Time and the law: International perspectives on an old problem' (1997) 46 *ICLQ* 501.

[113] See Karine Bannelier 'Foundational judgment or constructive myth? The court's decision as a precursor to international environmental law' in Karine Bannelier, Théodore Christakis and Sarah Heathcote (eds), *The ICJ and the Evolution of International Law. The Enduring Impact of the Corfu Channel Case* (Routledge 2012) 242–55.

the environment that prevailed in 1997.[114] Similarly, the Appellate Body of the World Trade Organization asserted that the Article XX(g) words 'exhaustible natural resources' should be interpreted not in a static manner, nor on the basis of the understanding that prevailed in 1947, but in a dynamic manner according to the understanding that prevailed in 1998.[115] In these cases, the judges did not want to adopt an interpretation that would have deprived the treaty of its effects. They interpreted these treaties in a teleological way so as to give full effect to their provisions. It is also well known that human rights treaty bodies constantly use evolutionary interpretation as a tool in order to 'adapt' and specify concepts and notions contained in human rights treaties in a rapidly evolving world. In the interests of protected persons these bodies have constant recourse to the idea that human rights treaties are 'living instruments', the interpretation of which inevitably requires a non-static process. As the former President of the European Court of Human Rights stated:

> The fact is that, more or less since the beginning, the Convention organs … have taken the view that the text should be interpreted, and applied, by adapting it to the changes that have taken place over time – to changes in society, in morals, in mentalities, in laws, but also to technological innovations and scientific progress. The Convention is sixty years old: history has moved inexorably onward during that period and this contextual evolution has been highly significant. The Convention's interpreters expressly rejected a static or finite analysis. I am convinced they were right.[116]

This dynamic approach to interpretation has always been part of the law of armed conflict as evidenced by the Martens Clause inserted in various treaties, or the famous Article 36 of Additional Protocol I. It is also due to this dynamic approach that cyber war is regarded as subject to the law of armed conflict. This is the same way that one should interpret Articles

---

[114] According to the Court:

> Owing to new scientific insights and to a growing awareness of the risks for mankind – for present and future generations –of pursuit of such interventions at an unconsidered and unabated pace, new norms and standards have been developed, set forth in a great number of instruments during last two decades. Such new norms have to be taken into consideration, and such new standards given proper weight, not only when States contemplate new activities but also when continuing with activities begun in the past

Gabčikovo-Nagymaros Project (Hungary/Slovakia) (Judgment) [1997] ICJ Rep 7, para 140. In the Case *Costa Rica v Nicaragua*, the ICJ, using a dynamic interpretation of a bilateral agreement concluded in1858, stated that 'Nicaragua, in adopting certain measures which have been challenged, in the Court's opinion, is pursuing the legitimate purpose of protecting the environment'; *Dispute Regarding Navigational and Related Rights (Costa Rica v Nicaragua)* (Judgment) [2009] ICJ Rep 213, para 89. See also Georg Nolte, 'Between contemporaries and evolutive interpretation: The use of subsequent practice in the judgment of the International Court of Justice concerning the case of Costa Rica v Nicaragua (2009)' in Holger P Hestermeyer (ed), *Coexistence, Cooperation and Solidarity: Liber Amicorum Rudiger Wolfrum* (vol II, Martinus Nijhoff 2012) 1675–84.

[115] According to the Appellate Body of the Dispute Settlement Body of the WTO:

> The words of Article XX(g), 'exhaustible natural resources', were actually crafted more than 50 years ago. They must be read by a treaty interpreter in the light of contemporary concerns of the community of nations about the protection and conservation of the environment. (...) the generic term 'natural resources' in Article XX(g) is not 'static' in its content or reference but is rather 'by definition, evolutionary'

WTO, *US: Import Prohibition of Certain Shrimp and Shrimp Products - Report of the Appellate Body* (12 October 1998) WT/DS58/AB/R paras 129–30.

[116] European Court of Human Rights, Council of Europe (eds), *Dialogue between Judges 2011: What are the Limits to the Evolutive Interpretation of the Convention?* (ECHR 2011) 5.

48 and 51 of Protocol I, taking into account that the objective of the drafters was to protect civilians from the effects of war. As Dinniss wrote:

> Once the ability to target civilian objects is permitted, it crosses the fundamental philosophical line enshrined in the 1868 Declaration of St Petersburg, which states 'the only legitimate object which States should endeavor to accomplish during war is to weaken the military forces of the enemy.[117]

In this context, it would be useful, taking into consideration the specificities of cyber warfare, to read the principle of distinction in accordance with its objective. This might refrain States from planning cyber operations that target civilians.

4. THE PROHIBITION OF INDISCRIMINATE ATTACKS IN CYBERSPACE

The prohibition of indiscriminate attacks raises numerous challenges in cyberspace that lie at the intersection between law and technology. Over the last few years, numerous cyber attacks carried out outside armed conflicts have shown that even State-sponsored attacks can have consequences far beyond their target, causing unexpected collateral damage to civilians around the world. This recurrence of collateral damage questions the very nature of these weapons: are they indiscriminate by nature, or is it rather the way that they are used that is indiscriminate **(**see section 4.a).

If, from a technical point of view, the development of cyberweapons that respect the principle of distinction is a complex task, the nature of cyberspace makes achieving distinction even more delicate. The principle of distinction implies that civilians and civilian objects can be clearly distinguished from combatants and military objectives. However, the distinction between civilians and civilian objects and military objectives, which had already been contextual at the time of the codification of the principle of distinction, has been gradually eroded. The 'civilianization'[118] of war has blurred the contours of these notions as illustrated by the success of the concept of *dual-use* objects which qualifies as military objectives civilian infrastructures serving partly a military function. The inextricable interconnectivity between the civilian and the military spheres that characterizes cyberspace pushes this trend to the limits by authorising attacks on an increasingly wide and diverse range of dual-use facilities (see section 4.b).[119]

This trend towards the 'civilianization' of war is not limited to objects and facilities, it also directly affects the civilian population. Indeed, cyber war depends largely on the technical expertise of civilians. This overuse of civilians in the military cyberspace raises questions whether they take a 'direct part' in hostilities. Undoubtedly, the interpretation of the notion

---

[117] Dinniss (n 26) 202.

[118] Andreas Wenger and Simon Mason, 'The civilianization of armed conflict: Trends and implications' (2008) 90 *IRRC* 835.

[119] As Vice Admiral Arthur Cebrowski highlighted, 'There is no logical distinction ... between military or civil systems or technologies. [Therefore] there is also no technical distinction between exploitation, attack or defense of the information warfare target set', quoted in Lawrence T Greenberg, Seymour E Goodman, Kevin J Soo Hoo, *Information Warfare and International Law* (National Defense University Press 1998) 12.

of direct participation in hostilities and the consequences of this participation constitute one of the most challenging questions in terms of how we apply the principle of distinction in cyberspace. It is therefore appropriate to clarify exactly when participation in military cyber operations qualifies as direct participation in hostilities (see section 4.c).

4(a) The Cyber Weapon: An Inherently Indiscriminate Weapon?

Prohibition of the use of weapons that are by their nature indiscriminate is widely recognized as a customary rule of IHL stemming from the general prohibition on indiscriminate attacks.[120] This rule applies 'to all forms of warfare and to all kinds of weapons'.[121] There is therefore no reason to exclude cyber weapons and cyber methods of warfare from the scope of this prohibition.

The US has perhaps one of the most advanced positions on this issue, making it clear publicly that cyber capabilities and cyber weapons should not be used indiscriminately.[122] But is it possible not to use cyber weapons indiscriminately? The answer is not set in stone since there is no single cyber weapon but a huge variety of them. As Wallace underlined, 'like their physical or kinetic counterparts, cyber weapons span a wide spectrum from specific, highly sophisticated weapons to more generic, less sophisticated ones'.[123] Among this variety of weapons, some are undoubtedly indiscriminate.

For example, malware that are self-replicating and/or self-propagating could qualify as indiscriminate. Certain countries, such as Denmark, France and the US have already tried to determine what would constitute an indiscriminate cyber weapon and hence be prohibited by IHL. Despite some differences amongst these countries, all three seek controllability: indiscriminate cyber weapons are cyber weapons that are uncontrollable. For the US, 'a destructive computer virus that was programmed to spread and destroy uncontrollably within civilian internet systems'[124] could qualify as indiscriminate. In the same way, France considers that '[t]he use of malware which deliberately reproduces and propagates with no possible control or reversibility, and is hence likely to cause significant damage to critical civilian systems or infrastructure, is contrary to IHL'.[125] For Denmark also, malware is indiscriminate when it 'creates an uncontrollable spill-over effect, including on a civilian digital infrastructure'.[126]

The question that needs to be asked therefore is whether it is possible to design cyber weapons that would not be indiscriminate. For many experts the answer is yes. According to them, cyber weapons do not self-propagate uncontrollably 'by chance', they have been

---

[120] ICRC, *Rule 71. Weapons that are by nature indiscriminate*, IHL Database, Customary rules, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule71.

[121] *Legality of the Threat or Use of Nuclear Weapons* (n 2) para 86.

[122] US Law of War Manual (n 15) 1025.

[123] David Wallace, "Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis", Tallinn Paper No. 11, Tallinn 2018, NATO CCD COE, https://ccdcoe.org/library/publications/cyber-weapon-reviews-under-international-humanitarian-law-a-critical-analysis/ p. 16.

[124] US Law of War Manual (n 15) 1025–6 and footnote referring to the *United States Submission to the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2012-2013*.

[125] Ministère des Armées (n 41) 16.

[126] Danish Ministry of Defence (n 45) 414.

deliberately designed to self-propagate.[127] The onus is therefore on States to tailor their cyber weapons so that propagation beyond their target is avoided. According to France:

> the risk of propagation beyond the target (…) may be contained by the development of specific cyber weapons whose use is decided according to the desired effects, determined beforehand (activation of malware only in the presence of a specific network previously identified by a penetration of the system, existence of a deactivation time, etc.).[128]

Accordingly, the ICRC underlined that '[c]yber operations can be tailored technically to specific targets, such as a country, a facility, a type of system or even individual user'.[129]

Logically therefore, this requirement implies that States are able to assess the effects of their cyber weapons in order to comply with the prohibition of indiscriminate weapons. For those who are party to Additional Protocol I, it is obviously clear that they must review the lawfulness of their cyber weapons in accordance with Article 36.[130] However, only a handful of State Parties to Additional Protocol I have publicly declared that their legal review of weapons includes cyber capabilities. One such State is Denmark.[131] Of course, this deafening silence has no bearing on the binding nature of Article 36 API with regard to cyber weapons, but this silence does have an impact on the customary nature of this obligation. To the author's knowledge, only the US, which is not a party to Additional Protocol I, has declared that it will conduct a legal review of cyber weapons.[132]

4(b) Distinguishing Between Civilian Objects and Military Objectives: The Problem of Dual-Use Objects in Cyberspace

For many States and experts,[133] distinguishing between civilian and military cyber infrastructure is a particularly challenging matter. As underlined by the UK, '[t]argeting can be challenging in cyber operations due to the potential dual use nature of some targets, such as infrastructure'.[134] This situation is even more challenging due to the fact that the law of war does not provide a clear definition of 'civilian objects'; it only provides a definition of military objectives. According to Article 52(2) of Additional Protocol I:

> Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effec-

---

[127] *International Humanitarian Law and Cyber Operations during Armed Conflicts* (n 22) 5.

[128] Ministère des Armées (n 41) 16.

[129] ICRC, 'The Potential Human Cost of Cyber Operations', ICRC Expert Meeting Geneva (14-16 November 2018) 55, https://www.icrc.org/fr/publication/potential-human-cost-cyber-operations.

[130] See on this question the detailed analysis of Mačák (n 94) 4–7.

[131] Danish Ministry of Defence (n 45) 380 and footnote 169.

[132] US Law of War Manual (n 15) 1025–6.

[133] See e.g., the analysis of Robin Geiss and Henning Lahmann, 'Cyber warfare: Applying the principle of distinction in an interconnected space' (2012) 45 *Israel Law Review* 381.

[134] United Kingdom, Ministry of Defence, *Cyber Primer* (2nd edn, 2015) 14, footnote 15. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf. See also *India's comments on the Initial Pre-Draft of the report of the OEWG on developments in the field of information and telecommunications in the context of international* security (April 2020) https://ccgdelhi.org/wp-content/uploads/2020/09/india-comments-on-oewg-2020-chair-pre-draft-final.pdf.

> tive contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.

Using *a contrario* reasoning, civilian objects are thus objects that *are not* military objectives. Depending on the circumstances and the necessities of war, the same object may be considered a civilian object, protected from attacks by the principle of distinction or a military objective 'which by their nature, location, purpose or use make an effective contribution to military action' and therefore subject to attack. Although this understanding is well established, interpretation of the two key elements of the definition remain subjective. As one commentator underlined: 'Although it seems that the principle of distinction between military and civilian objects is a straightforward principle, it is often difficult to apply in practice. The main ambiguity derives from different interpretations of the terms "effective" and "definite"'.[135]

Some authors[136] and some States have adopted a broad interpretation of the concept of military objective that profoundly undermines the principle of distinction. A well-known example of this is the *US Navy Commander's Handbook on the Law of Naval Operations*, according to which military objectives may include not only 'war-fighting' but also 'war-sustaining' installations. As it says:

> Military objectives are combatants and those objects which, by their nature, location, purpose or use effectively contribute to the enemy's war-fighting or war-sustaining capability and whose total or partial destruction, capture or neutralization would constitute a definite military advantage to the attacker under the circumstances at the time of attack.[137]

During NATO's airstrikes against Serbia in 1999, Lieutenant General Short of the NATO Air Component declared that it wanted to 'turn off the lights' of Belgrade.[138] The bombing in April 1999 of the Radio Television Serbia HQ was also presented as a military objective because it was seen as the central nervous system that kept Milošević in power.[139] At the same time, according to US military sources, 'bridges were often selected for attack for reasons other than

---

[135] Osnat Davidson, 'A legal analysis of computer network attacks under international law' (2007–2008) 3 *IDF L Rev* 70, 94

[136] This doctrinal trend is well illustrated by Dunlap, who argues for a new kind of total war, stating that:

> We need a new paradigm when using force against societies with malevolent propensities. We must hold at risk the very way of life that sustains their depredations, and we must threaten to destroy their world as they know it if they persist. This means the air weapon should be unleashed against entire new categories of property that current conceptions of LOAC put off-limits

Charles J Dunlap, 'The end of innocence: Rethinking non-combatancy in the post-Kosovo era' (2000) 28 *Strategic Rev* 9.

[137] Department of the Navy, Office of The Chief of Naval Operations, 'The Commander's Handbook on the Law of Naval Operations' (Edition July 2007) 8.2 (*Military Objectives*) http://www.usnwc.edu/getattachment/a9b8e92d-2c8d-4779-9925-0defea93325c/.

[138] Cited by Michael N Schmitt, 'The impact of high- and low-tech warfare on the principle of distinction' in Roberta Arnold and Pierre-Antoine Hildbrand (eds), *International Humanitarian Law and the 21st Century's Conflicts: Changes and Challenges* (Edis 2005).

[139] ICTY Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia (Jun 2000) 26, http://www.tpiy.org/x/file/About/OTP/otp_report_nato_bombing_en.pdf.

their role in transportation (for example, they were conduits for communications cables, or because they were symbolic and psychologically lucrative)'.[140]

But even though the notion of a 'war-sustaining' installation remains controversial, it is true that, for States, many facilities, such as electric grids, chemical plants, oil refineries, dams, bridges, telecommunications equipment or transport infrastructure could qualify as *dual-use objects* and could consequently be targeted during hostilities.[141] While some States seem reluctant to convert civil infrastructure into a military objective,[142] many experts consider that 'when a certain object is used for both military and civilian purposes, it may be held that even a secondary military use turns it into a military objective'.[143] In cyberspace and due to the nature and dual use of cyber objects, it may lead to more frequent findings of their military nature or use.

Moreover, the mere structure of cyber space, which is 'predominantly civilian in nature'[144] makes it difficult to segregate military from civilian objects[145] and to avoid the temptation to

---

[140] Quoted by Jeanne M Meyer, 'Tearing down the facade: A critical look at the current law on targeting the will of the enemy and air force doctrine' (2001) 51 *Air Force L Rev* 165.

[141] It is for example interesting to note that according to the 1954 *Convention for the Protection of Cultural Property in the Event of Armed Conflict*, broadcasting stations are military objectives. According to Art 8(1):

> There may be placed under special protection a limited number of refuges intended to shelter movable cultural property in the event of armed conflict, of centres containing monuments and other immovable cultural property of very great importance, provided that they: (a) are situated at an adequate distance from any large industrial centre or from any important military objective constituting a vulnerable point, such as, for example, an aerodrome, broadcasting station, establishment engaged upon work of national defence, a port or railway station of relative importance or a main line of communication.

[142] According to France, 'ICT infrastructure or a system used for both civilian and military purposes may, after detailed analysis on a case-by-case basis, be deemed a military objective'; Ministère des Armées (n 41) 15.

[143] Marco Sassòli, 'Legitimate targets of attacks under international humanitarian law' (Background Paper prepared for the Informal High-Level Expert Meeting on the Reaffirmation and Development of International Humanitarian Law, 27-29 January 2003) 7, http://www.hpcrresearch.org/sites/default/files/publications/Session1.

[144] ICRC, 'The Potential Human Cost of Cyber Operations', ICRC Expert Meeting, Geneva, 14–16 November 2018, 32, https://www.icrc.org/fr/publication/potential-human-cost-cyber-operations. According to this report, '[c]yber space is probably a 90% civilian build and owned infrastructure' (33) and as underlined the ICRC in its position paper of 2019;

> [e]xcept for some specific military networks, cyberspace is predominantly used for civilian purposes. However, civilian and military networks may be interconnected. Furthermore, military networks may rely on civilian cyber infrastructure, such as undersea fibre-optic cables, satellites, routers or nodes. Conversely, civilian vehicles, shipping and air traffic controls increasingly rely on navigation satellite systems that may also be used by the military. Civilian logistical supply chains and essential civilian services use the same web and communication networks through which some military communications pass.

International Humanitarian Law and Cyber Operations during Armed Conflicts (n 22) 6.

[145] According to the Tallinn Manual;

> [i]t may not always be feasible for parties to a conflict to segregate potential military objectives from civilian objects. For example, a power generation plant or an air traffic control center may serve both military and civilian purposes. Civilians and civilian objects might be present at these lawful targets and it may not be feasible to segregate them in accordance with this Rule. Similarly, it might be impossible to segregate the civilian and military functions of the infrastructure.

Tallinn Manual 2.0 (n 37) 489.

treat all such objects as military. As Droege has said, 'in cyber space the consequences could be exacerbated to an extreme point where nothing civilian remain'.[146] For instance, according to commentators, civilian servers that are used to transmit military information *are* military objectives.[147]

In this regard, the status of computers and computer systems, and companies associated with these systems, calls for special attention. Since computer systems are at the heart of modern armies they can be considered 'war-fighting' and therefore military objectives. But what about the companies that design and produce hardware or software? Are they dual-use entities and, as such, could they be military targets? According to the Tallinn Manual, '[a]n object used for both civilian and military purposes-including computers, computer networks and cyber infrastructure-is a military objective'.[148] Is it possible that Apple, Microsoft, IBM or Dell might become targets as war-sustaining installations?[149]

Aside from these companies, could the internet and/or social media companies, such as Facebook or Twitter, become military objectives? Already in 1995, 95 per cent of the Department of Defense's telecommunications were directed through the Public Switched Network,[150] and today social media is of enormous importance to many armed groups.[151] Could it be possible to consider that they 'make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage'? France for example maintains that 'a propaganda center may be a lawful military objective and the target of a cyberattack if it disseminates instructions linked to the conduct of hostilities'.[152] Other States seem to go way beyond this, seeing the whole of the internet as a dual-use object. For example, President Bashar al-Assad of Syria allegedly interrupted access to the internet in order to cripple the communication abilities of rebel forces.[153]

Even if one is reluctant to view the internet as a global military objective based on the idea that only 'segments' of the internet used for military purposes should be targeted,[154] the interconnection between civilian and military networks is so deep that an attack that is strictly limited or 'proportional' seems in many cases rather illusory. Apart from the fact that it can be difficult to identify the segments used for military purposes, the mere fact of introducing a virus into a military network or into a military objective via a civilian network can have effects that go far beyond the military framework.[155]

---

[146] Droege (n 39) 565.

[147] Schmitt (n 107) 27.

[148] Tallinn Manual 2.0 (n 37) 445.

[149] See e.g., Eric Talbot Jensen, 'Unexpected consequences from knock-on effects: a different standard for computer network operations?' (2002) 18 *American University Intl L Rev* 1544.

[150] Richard W Aldrich, 'The International Legal Implications of Information Warfare' (US Air Force Institute for National Security Studies Occasional Paper 9, April 1996) 11.

[151] See examples of Nepal, Myanmar or Egypt given by Dinniss (n 26) 186.

[152] Ministère des Armées (n 41) 14.

[153] Chris Finan, 'A cyberattack campaign for Syria', *The International Herald Tribune* (27 May 2013).

[154] Tallinn Manual 2.0 (n 37) 446.

[155] The Stuxnet experience shows that 'although the worm was designed against Iranian's nuclear power plant, its spread infected 45 000 computers around the world': Thomas Erdbrink and Ellen Nakashima, 'Iran struggling to contain 'foreign-made' computer worm', *The Washington Post Staff* (28 September 2010).

4(c) The Protection of Civilians and the Problem of Direct Participation in Cyber Hostilities

The fate of those involved in cyber operations is undoubtedly one of the most complex issues faced by the law of armed conflict. The principle of distinction assumes that belligerents can clearly distinguish between civilians and combatants. However, for various reasons, armed forces are increasingly using civilians to perform a wide range of activities in connection with military cyber operations. This information technology outsourcing includes military network maintenance, exploitation of computer system weaknesses and the development and instillation of worms, Trojan horses and other viruses. According to Turns: 'In light of these trends, there is a high probability that many, if not most, of the personnel substantively involved in cyber-operations may actually be civilians.'[156]

What then is the status of the experts involved in these cyber operations? The protection against attacks afforded to civilians by the principle of distinction is subject to the fundamental requirement that civilians do not directly participate in hostilities.[157] This presumption of 'innocence' is inserted into most provisions relating to the principle of distinction and the protection of civilians.[158] For example, according to Article 51(3) of Protocol I: 'Civilians shall enjoy the protection afforded by this Section, unless and for such time as they take a direct part in hostilities.' In this case, people that take direct part in hostilities could become the target of attacks. Could a hacker or computer scientist therefore become the object of an attack? The answer to these questions depends on how we interpret the notion of 'direct participation in hostilities' when cyber operations are concerned.

In this regard, the *Interpretive Guidance on the Notion of Direct Participation in Hostilities* published by the ICRC is helpful.[159] Although some of its proposals remain controversial, the main conclusions of this document seem to garner consent, and call for at least two sets of observations in relation to cyber operations.

The first set of observations concerns the meaning of the notion of 'direct participation in hostilities' in the context of cyberwarfare. First, it is interesting to note that the notion of 'hostility' has been interpreted widely enough to encompass a large variety of acts. According to the ICRC's Interpretive Guidance, 'there was wide agreement that the causation of military harm as part of the hostilities did not necessarily presuppose the use of armed force or the causation of death, injury or destruction', but essentially included 'all acts that adversely affect or aim to adversely affect the enemy's pursuance of its military objective or goal'.[160] In other words, 'hostilities' is not synonymous with attacks and cyber military operations that are

---

[156] Turns (n 64) 292.

[157] Claude Pilloud, *Commentaires des Protocoles additionnels du 8 juin 1977 aux Conventions de Genève du 12 août 1949,* (Martinus Nijhoff Publishers 1986) 633.

[158] See e.g., common art 3 to the four *Geneva Convention of 12 August 1949*; art. 13(3) of *Protocol Additional to the Geneva Conventions of 12 August 1949 relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II)*, 8 June 1977*;* art 38 of the *Convention on the Rights of the Child* of 20 November 1989; art 1 of the *Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict*, 25 May 2000; art 8.2(b)(i) and 8.2(e)(i) of the *Rome Statute of the International Criminal Court*, 17 July 1998.

[159] Niels Melzer (ed), *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (ICRC 2009) 85.

[160] Ibid., 14, 22–31.

below the threshold of an attack could be qualified as 'hostilities'. According to the Tallinn Manual, '[t]here is no requirement for physical damage to objects or harm to individuals. In other words, actions that do not qualify as a cyber-attack will satisfy this criterion as long as they negatively affect the enemy militarily'.[161] From this point of view, it can be concluded that a wide range of cyber operations could fall under the scope of 'hostilities'.

However, in order to determine that an act involves 'direct participation', three additional requirements should be met: '(1) a threshold regarding the harm likely to result from the act; (2) a relationship of direct causation between the act and the expected harm; and (3) a belligerent nexus between the act and the hostilities conducted between the parties to an armed conflict'.[162] Here again, although these criteria are cumulative, it seems that a broad range of cyber activities could fit the definition. According to the ICRC Interpretive Guidance, '[e]lectronic interference with military computer networks could also suffice, whether through computer network attacks (CNA) or computer network exploitation (CNE), as well as wiretapping the adversary's high command or transmitting tactical targeting information for an attack'.[163] States that have made declarations about this issue seem to be following the same interpretation. France, for example, opined that 'the penetration of a military system by a party to an armed conflict with a view to gathering tactical intelligence for the benefit of an adversary for the purposes of an attack constitutes direct participation in hostilities. The same applies to installing malicious code, preparing a botnet in order to launch an attack by denial of service, or developing software specifically intended for the perpetration of a hostile act'.[164]

This could therefore lead us to the preliminary conclusion that many civilians involved in military cyber operations could meet the criteria of 'direct participation in hostilities', 'even if they do not actually press the button that launches a cyber-attack'.[165]

The second set of observations concerns the effects of civilians' participation in cyber hostilities on their protective status. The fact that civilians could be a legitimate target and might be the subject of an attack (cyber or kinetic) has been confirmed.

Nevertheless, the interpretation of the expression 'for such time' in the context of cyberwarfare is particularly challenging and needs clarification. Indeed, should civilians only be targeted once they 'press the button', or can they only be targeted once the cyber operation is under way? As Schmitt rightly underlined:

> This is problematic in that many cyber operations last mere minutes, perhaps only seconds. Such a requirement would effectively extinguish the right to strike at direct participants. Moreover, the effect of a cyber-operation may be long-delayed, as in the case of a surreptitiously emplaced logic bomb. Would the target of such an operation only be entitled to attack the direct participant while the logic bomb is being emplaced?[166]

---

[161] Tallinn Manual 2.0 (n 37) 429 (Rule 97 Civilian Direct Participants in Hostilities).

[162] Melzer (n 159) 46. For a detailed analysis in the context of cyberwarfare see David Wallace, Shane Reeves and Trent Powell, 'Direct participations in hostilities in the age of cyber: Exploring the fault lines' (2021) 12 *Harvard National Security Journal* 164.

[163] Melzer (n 159) 48.

[164] Ministère des Armées (n 41) 15.

[165] Quoted by Turns (n 64) 290.

[166] Schmitt (n 78) 102.

On the other hand, it could be extremely dangerous to adopt too broad an interpretation and to consider that it is permissible to launch attacks against these civilians as long as the effects of their actions are apparent. To quote Schmitt again: 'In the cyber conflict environment, therefore, the only reasonable interpretation of "for such time" is that it encompasses the entire period during which the direct cyber participant is engaging in repeated cyber-operations'.[167] Balanced and reasonable as it might be, this interpretation does not resolve all the problems.

For example, should we consider the replication of a worm as a 'repeated cyber-operation'? If we do, then the time scale of direct participation in hostilities will extend exponentially. But if the answer to this question is no, when can we say that said cyber operation is over?

The ubiquity of cyber operations is also extremely challenging. Indeed, cyber operations can be launched simultaneously by thousands of computers all around the world and the instigators of these operations can be located in civilian areas far away from the 'battlefield' (if there are any battlefields at all). The principle of distinction prohibits indiscriminate attacks but authorises lethal attacks against civilians who directly participate in hostilities, including collateral damage to civilians and civilian objects. The caveat here is that these damages are not excessive in relation to the specific military advantage anticipated.[168]

In this context, one may wonder whether the notion of direct participation in hostilities in cyberspace could become a kind of Trojan horse (or worm) that infiltrates the principle of distinction leading to a kind of 'total cyber war'.[169] The risks of abuse are however not so obvious. Indeed, as we have discussed previously, the three criteria for direct participation are cumulative, bringing the threshold requirement to a fairly high level. In addition, the second direct participation criterion requires 'a relationship of direct causation between the act and the expected harm' which is difficult to establish in the context of cyber war as shown previously. As Turns noted: 'In these circumstances, it appears doubtful that CW [cyber warfare] could ever meet the requirement of direct causation for DPH [direct participation in hostilities], which suggests that civilians could engage in CW [cyber warfare] with impunity.'[170]

5. CONCLUSION

As the preceding discussion has demonstrated, the prevailing view that cyberwarfare is subject to the law of armed conflict and more specifically to the principle of distinction is accurate. However, this view should not overshadow the difficulties involved in interpreting and applying the principle of distinction to cyberwarfare. Of course, the difficulties in applying the principle of distinction 'in the heat of battle' are not new, but cyber war stretches them further. For the time being, our knowledge of how this principle applies to cyber warfare is very limited due to lack of practice and therefore the risks we highlighted in this chapter remain somewhat theoretical, albeit realistic. One should however follow closely future developments which could indicate how this old 'cardinal' and 'intransgressible' principle will be interpreted and applied in the cyber battlefield.

---

[167] Ibid.

[168] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (8 June 1977) (Protocol I), art 51(5)(b).

[169] Droege (n 39) 565.

[170] Turns (n 64) 288.

21. International humanitarian law applied to cyber-warfare: precautions, proportionality and the notion of 'attack' under the humanitarian law of armed conflict

Terry D. Gill

1. INTRODUCTION

The applicability of international law to 'cyber-warfare' has received significant attention in recent years. A number of States have presented (semi) official positions on the question of the applicability of international law to cyber-warfare and several noteworthy publications have appeared in which the applicability and application of international law to cyber attacks and other forms of cyber activity have received attention. These include the *Tallinn Manual* on cyber warfare and the follow-up edition including peacetime cyber activity known as *Tallinn 2.0*, along with other publications including the first edition of this Research Handbook and many more too numerous to name.[1] Alongside the applicability to cyber warfare of the *ius ad bellum* governing the permissibility of the use of force and the conditions and modalities relating to its application in response to cyber attacks, the question of the applicability of the *ius in bello*, generally referred to as International Humanitarian Law or the Law of Armed

[1] For examples of State positions on cyber-warfare and the applicability of international law thereto see, Michael N Schmitt (ed), *Tallinn Manual on the Applicability of International Law to Cyber Warfare* (CUP 2013) 2 (hereinafter referred to as Tallinn Manual), citing the national cyber strategies of, *inter alia*, Canada, the Russian Federation, the United Kingdom and the United States. The Netherlands also adopted a position which endorsed the findings of the Advisory Council for International Affairs and the Advisory Committee on Matters of Public International Law Report on Digital Warfare issued in 2011 in which it acknowledged that existing international law, including the law relating to the use of force and international humanitarian law, fully apply to cyber-warfare. See for the joint report of the two bodies AIV/CAVV Report 77/22, *Cyber Warfare*, December 2011 available online http://www.aiv-advies.nl/ContentSuite/upload/aiv/doc/webversie__AIV77CAVV_22_ENG.pdf. For the Dutch Government's response, see http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/04/26/cavv-advies-nr-22-bijlage-regeringsreactie-en/cavv-advies-22-bijlage-regeringsreactie-en.pdf. France recently updated its national cyber defence strategy in a publication by the Ministry of Defence, 'International Law Applicable to Operations in Cyberspace' issued in December 2019 see https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/. Alongside State reactions, a considerable amount of literature has appeared devoting attention to the international legal aspects of cyber-warfare, both in relation to use of force issues and the application of IHL/LOAC These are too numerous to name, but a few examples of some noteworthy publications will serve to illustrate. Among these publications are (2012) 17 *J of Conflict and Security L* devoted wholly to cyber-warfare; Paul Ducheine, Frans Osinga and Joseph Soeters (eds), *Cyber Warfare: Critical Perspectives* (TMC Asser Press 2012); (2013) a series of articles published in 89 *Intl L Studies*; and the publications of the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), including the aforementioned Tallinn Manual.

Conflict (IHL/LOAC), has also received attention, albeit probably somewhat less on the whole in relation to cyber attacks, than the law governing the use of force. Both aspects are, however, dealt with in the aforementioned *Tallinn Manual*. In this chapter, I will set out some of the main positions put forward in that study and elsewhere relating to the application of IHL to cyber hostilities and offer some personal views in relation to the question to what extent this body of law is relevant and applicable to 'cyber warfare'. In that context, I will devote specific attention to when, under which circumstances and how the rules of humanitarian law relating to the conducting of attacks, with a focus on proportionality, would apply to hostilities carried out wholly or partially in the cyber domain.

This chapter is based on several premises, which however obvious some may seem, need emphasizing. First, that as a matter of law, IHL/LOAC only applies when the conditions relating to the threshold of the existence of an armed conflict have been reached. Secondly, that to date, there has never been a single instance of a 'stand-alone' cyber attack or other act of cyber interference or sabotage, which has come close to meeting that threshold. Thirdly, that the likelihood of such a 'stand -alone' cyber attack reaching that threshold is remote at best.[2] Fourthly, and consequently, that if IHL/LOAC is applicable to 'cyber-warfare', it will most likely be in the context of a 'regular' armed conflict in which cyber operations are conducted alongside traditional 'kinetic' attacks involving the application of IHL/LOAC to the entire spectrum of operations and attacks which are conducted by any party to the conflict. Fifthly and finally, that any armed conflict, irrespective of the means and methods of warfare employed, is subject to the rules and principles of international humanitarian law, and these rules are equally applicable to any party to such a conflict.[3]

This chapter is structured as follows. In the following section, a few considerations will be set out in support of the premises presented above. In the third section, the rules of IHL/LOAC relating to the notion of 'attack', the taking of precautions to spare the civilian population and civilian objects and the duty to conduct such attacks in conformity with the principle of proportionality (as it applies within IHL/LOAC) will be briefly set out. In the fourth section, these rules will be applied in the context of cyber attacks conducted within the context of an armed conflict. In the fifth and final section, a number of conclusions will be presented.

2. WHY AND WHEN HUMANITARIAN LAW WOULD OR WOULD NOT APPLY TO 'CYBER-WARFARE'

The starting point of this explanation of the premises underlying this chapter is that IHL/LOAC is a legal regime which only applies if there is in fact an armed conflict of either an international or non-international character. The qualitative threshold for international armed conflict is provided for in common Article 2 of the Geneva Conventions of 1949 and is restated authoritatively in case law. Although some doubt may arise as to the applicability of all the rules of IHL treaty and customary law in relation to isolated, small-scale incidents involving incidental clashes between the armed forces of two States, it is well established that

---

[2] Thomas Rid, 'Cyber war will not take place' in Ducheine, Osinga and Soeters (n 1) 73.

[3] This follows from the ICJ's statement that international humanitarian law applies to all weapons (past, present, and future weapons) in the context of an armed conflict; see *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226, para 39.

an international armed conflict exists when there is a conflict between the armed forces of two or more States and/or a total or partial occupation of the territory of a State by another State, irrespective of whether there is armed resistance to such occupation, a situation of declared or factual war, or greater or lesser loss of life and injury, and damage and destruction.[4] In short, any armed clash above the most inconsequential between two or more States results in the existence of an international armed conflict and the applicability of IHL/LOAC to the parties. With regard to non-international armed conflicts, the situation is not as sharply defined, but on the basis of widely accepted criteria set out in the case law of the International Criminal Tribunal for the Former Yugoslavia relating to the requisite degree of organization, intensity and duration, a non-international armed conflict exists when there are armed clashes of an intensity and duration between an organized armed group and a State, or between two or more organized armed groups, which rise above the level of unorganized or sporadic armed violence or civil unrest.[5] If these criteria are met, the rules and principles of IHL/LOAC relating to non-international armed conflict apply to the parties to the conflict, irrespective of how the conflict is characterized by either party. Anything below either of these thresholds is not an armed conflict in the legal sense and IHL/LOAC does not apply as a matter of law, even though either party may elect to apply certain of its rules as a matter of policy.

Although the geographical scope of armed conflict is not the focus of this contribution, it deserves mention that in an international armed conflict (i.e. between two or more States) IHL/LOAC is applicable throughout the territory of any and all States party to the conflict and in international sea and airspace to the extent military operations are conducted there. The territory of third States is inviolable unless one of the parties conducts military operations from the territory of a non-belligerent (neutral) State and that State fails to uphold its duties as a neutral to prevent and put an end to such operations.[6] In non-international armed conflicts, IHL/LOAC applies within the territory of the State in question. It will only apply to the territory of a third State to the extent an armed group (partially) relocates to the territory of a third State and conducts operations from there, without the government of that State taking necessary and adequate measures to prevent or halt such operations being conducted from its territory.[7] The

---

[4] Common art 2 of the Geneva Conventions of 1949, reaffirmed in, inter alia, Jean Pictet (ed), *Commentary to the First Geneva Convention for the Amelioration of the Condition of the Wounded and the Sick in Armed Forces in the Field* (1952) 32. See also *Prosecutor v Dusko Tadić* (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) [1995] No ICTY-94-1-A para 70. For discussion whether an international armed conflict results from an isolated low-level armed incident, see, Christopher Greenwood, 'Scope of application of humanitarian law' in Dieter Fleck (ed), *The Handbook of International Humanitarian Law* (OUP 2008) 48.

[5] *Prosecutor v Dusko Tadić* (n 4) para 20; *Prosecutor v. Ramush Haradinaj et.al.* (Judgement) [2008] IT-04-84-T para 60. On the qualification of cyber armed conflict see Arimatsu (Ch 19 of this Handbook).

[6] For the geographic scope of international armed conflict, see e.g. Greenwood (n 4) 59–62; on neutrality law as it applies under the UN Charter, see e.g. Michael Bothe 'The law of neutrality' in Fleck (n 4) 571 *et seq* 582–3.

[7] The normal situation is that non-international armed conflicts occur within the territory of the State in question. In some cases, there is 'spill-over' of a non-international conflict onto the territory of one or more other States whence operations are conducted rising to the level of non-international armed conflict, see, inter alia, Tallinn Manual (n 1) rule 21 (Rule 81 T.2.0) and accompanying commentary 78–9. An example of such a spill-over is the conflict between Iraq supported by an international coalition and the ISIS armed group between 2014 and early 2020 with ISIS operating from its former base of operations in North Syria over the border deep into Iraq at one point controlling a significant portion of

result in both cases is that barring exceptional circumstances, the territory of States not party to the armed conflict is inviolable. In relation to international armed conflicts, this is due to the law of neutrality, alongside rules of general international law relating to State sovereignty and in relation to non-international armed conflicts, due to the latter set of rules arising from principles of State sovereignty and non-intervention, alongside rules and principles arising from the *ius ad bellum*.[8]

Stand-alone cyber attacks have, to date, never met either of these thresholds for the existence of an armed conflict. No example of cyber espionage, interference, intellectual property theft, or even sabotage has until now even approached the threshold of either an international or non-international armed conflict.[9] As serious as cyber espionage, cyber interference and cyber theft and crime are, they are not 'warfare' in anything but a semantic sense. Even when States engage in massive cyber surveillance and espionage, cyber intellectual property theft, cyber interference and cyber non-armed intervention, the lawful responses are to be found in the law relating to law enforcement, retorsion and countermeasures, and not the law relating to the use of force or the humanitarian law of armed conflict. Likewise, cyber terrorism would not automatically trigger the applicability of IHL/LOAC. This would only occur if it resulted in the threshold of either an international or non-international armed conflict, as set out above, being met. There has been, to date, no such example of cyber terrorism, but its occurrence at some point in the future cannot be ruled out. If the necessary conditions relating to the degree of organization, intensity and duration were present, this could result in the applicability of IHL/LOAC, but despite fears of such cyber terrorism, it would seem unlikely that a terrorist group would resort to cyber means instead of the type of terrorist attacks that have been used and are being used by such groups on a regular basis. This is because cyber vulnerabilities are

---

Iraqi territory for a period of several years and with the international coalition supporting Iraq conducting airstrikes against ISIS in both Iraq and in then ISIS controlled areas in North Syria. While opinions differ on whether and at what point an armed conflict between Syria and members of the anti-ISIS coalition may have resulted as a consequence of military action on Syrian territory, there is general agreement that there was a 'spill-over NIAC' in progress between Iraq and the coalition on the one hand and ISIS on the other during that period of time. See e.g. RULAC (Geneva) at http://www.rulac.org/browse/conflicts/non-international-armed-conflicts-in-syria.

[8] The relevance of the principles of sovereignty, non-intervention and the prohibition of the use of force to this question is self-evident. In addition, international law regulating self-defence, while not unanimous in State practice and academic opinion, shows considerable support for the possibility of conducting self-defence in response to armed attack from across an international frontier by a non-State organized armed group if the State from where the attack originated either controls or exercises substantial involvement in the attack, or when a necessity of self-defence otherwise arises often because the State where the armed group is operating is unable or unwilling to prevent such attacks being conducted from its territory. This can lead to a situation where there is an overriding necessity to counter such attacks when other measures are not available or would not suffice to end the ongoing or impending attack. The existence of an armed attack and the lack of feasible alternatives for ending the attack are the key components of the principle of necessity within self-defence, which is the bedrock requirement for its exercise. Only when the State where the operations are conducted from fails to take adequate measures to prevent attacks being mounted from its territory, is there a potential necessity to take action in self-defence. To the extent these operations rise to the level of a non-international armed conflict, humanitarian law relating to such conflicts would become applicable. See, inter alia, Tallinn Manual ibid., 58–9 and 61–6. For further discussion on self-defence in relation to non-State actors see, Terry D Gill and Kinga Tibori-Szabo, 'Twelve key questions on self-defense against non-state actors' (2019) 95 *International Law Studies* 467.

[9] Rid (n 2) 75 et seq.

almost certainly overstated on the one hand and on the other hand, the necessary economic, financial and technical resources to achieve massive societal dislocation on a long-term basis or inflict large-scale casualties by cyber means alone are not readily available to most, if any, terrorist groups.[10]

Neither is it likely, in the event of an armed conflict between States, that massive stand-alone cyber attacks, sometimes referred to as 'cyber Pearl Harbour' scenarios, would be the most likely way in which hostilities were conducted under such circumstances. In the event a large-scale armed offensive were carried out by a State against another State, it would seem illogical that such an attack would be confined to cyber means of warfare. Under such circumstances, the State conducting such an offensive would be most likely to utilize all means of warfare at its disposal. If one decides to conduct all-out warfare for whatever reason, why limit oneself to one weapon alone?[11] Nor is it much more likely that a smaller scale armed attack against a discrete target would be conducted by cyber means alone. The reasons for this are basically twofold. First, such a stand-alone cyber armed attack would not ensure the destruction or effective elimination of the target permanently, or for a prolonged period. If, for example, one wished to take out a particular military capability, platform or critical installation, it would be exceedingly difficult to ensure long-term effective damage, destruction or degrading of the targeted object by cyber means alone. In such a case, cyber techniques of warfare would be much more effective if used in conjunction with traditional 'kinetic' weapons, as was the case in the Israeli attack on the Syrian nuclear reactor in September 2007, when cyber techniques akin to electronic jamming were reportedly used as a means to temporarily neutralize Syrian air defences in order to clear the way for Israeli fighter bombers to attack and destroy the nuclear installation in northern Syria.[12] If, on the other hand, one wished to remain undetected (at least initially) and below the threshold of an armed attack in order to gather intelligence or inflict mere sabotage upon a system, as in the case of the *Stuxnet* sabotage of Iranian nuclear centrifuges, the threshold of an armed attack or of an armed conflict, would not be met. In short, cyber means of surveillance, espionage and sabotage are used regularly by a variety of actors without this being deemed to constitute 'warfare' in either the factual or legal sense.[13]

Consequently, the most likely way in which cyber means and methods of warfare would be used within the context of an armed conflict, aside from intelligence gathering and conducting counter-intelligence and various types of information operations, such as psychological warfare or the influencing of public opinion, would be as an adjunct and assist to attacks conducted by traditional means, as was the case in the aforementioned example of the Israeli airstrike on the Syrian reactor. In such circumstances, cyber operations are essentially another form of electronic warfare, which has been around for a considerable amount of time. The most likely employment would be within the context of operations directed against the adversary's 'sensory and nervous systems', such as degrading command, control and commu-

---

[10] Sean Lawson, 'Beyond cyber-doom: Cyber attack scenarios and the evidence of history' (2012) 10 *J of Information Technology and Politics* 1, 4.

[11] Chinese military strategy is often cited as an example of how cyber methods would likely be used in conjunction with traditional force in the event of any war between the PRC and another State, see Han Bouwmeester, Hans Folmer and Paul Ducheine, 'Cyber security and policy responses' in Ducheine, Osinga and *Soeters* (n 1) 34–7.

[12] Rid (n 2) 84–5. See also Terry D Gill and Paul Ducheine, 'Anticipatory self-defence in the cyber context' (2013) 89 *Intl L Studies* 438, 461–2.

[13] Ibid. 459; Rid (n 2) 85–8.

nications systems, weapons guidance systems, and detection systems like radar systems. This would almost always be conducted alongside more traditional means and methods of warfare, and as such, would be subject to IHL/LOAC rules and principles, including those pertaining to the conducting of 'attacks', whenever such operations amounted to 'acts of violence directed against the adversary, whether in offense or defence',[14] which were reasonably likely to result in physical damage, destruction, death or injury. Hence, while it is quite possible and even likely that cyber-warfare in the real sense of the word will occur at some point, it is most likely to occur in a fairly traditional battle space, both physical and electronic, in which a variety of means and methods of warfare are employed alongside each other, including certain techniques of digital warfare. Because of the resources required to successfully design and employ cyber weapons and the types of operations in which they would be most likely used and most effective, it seems probable that most cyber-warfare in the real sense would occur within the context of international (inter-State) armed conflicts, since most armed groups do not have either the resources, or the type of sophisticated command, control, communications and weapons systems which would make the techniques of cyber-warfare a logical choice of means. If this is a correct surmise, without necessarily ruling out other possible scenarios categorically, then it equally logically follows that whenever such an armed conflict occurs, it will be governed and regulated by the rules and principles of IHL/LOAC which pertain to the conduct of hostilities, including the principle of proportionality in the conducting of 'attacks' which are likely to affect the civilian population, since they apply to all weapons and targeting in any armed conflict. We will therefore now turn to the law which is relevant to such attacks.

3. THE LAW OF ARMED CONFLICT RELATING TO THE CONDUCTING OF ATTACKS

The law relating to the conduct of attacks within IHL/LOAC is primarily contained in Articles 48–58 of the First Additional Protocol to the Geneva Conventions of 1949 (hereinafter referred to as AP I.) While this only applies as treaty law to parties to AP I, which is applicable in international armed conflicts, the customary law relating to the conduct of attacks is substantially similar and binds all States and parties to armed conflict, and is applicable in all armed conflicts whether international or non-international in character.[15] For the sake of simplicity, the relevant provision of AP I will be cited where necessary, when referring to a specific rule or rules.

---

[14] This is the definition of attack under IHL/LOAC as stated in First Additional Protocol to the Geneva Conventions of 1949 (AP I) art 49 and under customary law.

[15] There are at present 174 States Party to AP I. Many, indeed most, of its provisions apply as customary law to non-parties in international armed conflicts and to all parties (both States and non-State armed groups) to non-international armed conflicts, alongside its binding effect upon State Parties to it in international armed conflicts as a matter of treaty law. The provisions of AP I relating to the conduct of attacks which have obtained customary status are reflected in the ICRC customary law study (ICRC CLS), which, notwithstanding certain criticism and shortcomings, has a widely recognized authoritative, but not binding status. For the purposes of this chapter, those rules will be assumed to reflect customary law, since a detailed examination falls outside its scope. The rules in the ICRC CLS relating to attacks are contained in rules 1–24 thereof.

The two main principles of IHL/LOAC in relation to the targeting of persons or objects subject to attack in an armed conflict are distinction and proportionality. These principles act alongside the two main principles of IHL/LOAC which are military necessity and humanity and several other principles, such as the principle of honourable conduct prohibiting perfidy in attacks and the principle of equal application of IHL/LOAC to all parties to the conflict, which form the core structure of this branch of international law.[16] The basic rules relating to the targeting of persons and objects are essentially the following: First, attacks may only be conducted against combatant members of the adversary's forces and military objectives.[17] These include regular members of the armed forces, with the exception of non-combatant military personnel (medical personnel and chaplains), or in non-international conflicts against fighting members of armed groups.[18] In addition, civilians directly participating in hostilities are subject to attack for the duration of their participation, including the period of deployment to and from the place where the attack is conducted.[19] Military objectives are those objects which according to their nature, use, purpose or location make an effective contribution to military operations and whose capture, destruction or neutralization would confer a definite military advantage under the circumstances prevailing at the time an attack is being considered or conducted.[20] Attacks may never be conducted against civilians, civilian objects, protected persons or objects, as such, unless they are directly participating in hostilities or have been converted into military objectives, in which case they lose their protection against attack.[21]

Secondly, in any attack that is likely to affect civilians or civilian objects, the principle of proportionality (as it applies within IHL/LOAC) must be observed. This provides that an attack which is likely to cause excessive civilian casualties or damage or destruction of civilian objects in relation to the concrete and direct anticipated military advantage expected from the attack (viewed a whole) is prohibited.[22] It should be noted that proportionality within IHL/LOAC is only relevant in an attack upon a military objective (including enemy personnel) which is likely to affect the civilian population or civilian objects. An attack which is not likely to affect civilians or civilian objects is not affected by this principle, while an attack deliberately directed against civilians or a civilian object, as such, is strictly prohibited and would constitute a war crime.[23]

---

[16] See e.g. UK Manual on the Law of Armed Conflict (JSP 383 (2004) Chapter 2, 21–6; US Dept. of Defense Law of War Manual 2015 updated December 2016, Chapter II. 50–69.

[17] AP I (n 14) art 49. On distinction in cyberspace see Bannelier (Ch 20 of this Handbook).

[18] Ibid. art 43 and ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law (26 February 2009) (IG DPH) 32–3.

[19] Ibid., 65.

[20] AP I (n 14) art 52:2.

[21] Ibid., art 51.

[22] Ibid., art 51:5 lit.b.

[23] The applicability of the principle of proportionality to attacks upon military objectives which are likely to affect civilians is clear from the text of art 51:5 lit.b and the scope of the section of AP I in which it appears and is related to protection of the *civilian* population. The weighing of military advantage against likely incidental and collateral effects upon civilians and civilian objects makes this completely clear. Likewise, since proportionality is only relevant in attacks upon military objectives whereby civilians may be affected and attacks against civilians and civilian objects, as such, are prohibited irrespective of any military advantage they might confer, proportionality is only relevant in relation to attacks upon military objectives whereby civilians are likely to be affected. Deliberate attacks upon civilians, as such, are simply prohibited as indiscriminate attacks. Both deliberate attacks upon civilians and dispropor-

Thirdly, constant care must be undertaken to spare the civilian population as far as possible and to prevent, or in any case, minimize loss of civilian life, injury of civilians and damage or destruction of civilian objects resulting from an attack on a military objective. This requires the taking of all feasible precautions when planning and conducting an attack and cancelling or suspending an attack whenever the collateral effects of the attack are likely to be excessive in relation to the concrete and direct military advantage anticipated. This is proportionality in a somewhat different context, namely in choosing the time, method and means of attack least likely to cause excessive collateral injury or damage. The standard here is that of the 'reasonable commander/combatant' acting in good faith and on the basis of information reasonably available at the time the attack is planned or conducted. It also requires an ongoing assessment as to whether the attack remains within the bounds of proportionality at all stages of the attack. Whenever possible, prior warning must be given to civilians likely to be affected, unless this would completely or largely compromise the attack.[24]

Fourthly, means (weapons) and methods of attack which are not or cannot be directed against a specific military objective or objectives or whose effects cannot be limited to military objectives and are consequently indiscriminate are prohibited. Hence means and methods of attack which cannot discriminate between military objectives and civilians and civilian objects are prohibited. Examples of this would be a weapon such as a ballistic missile without a reliable guidance system, such as the Scud missiles used by Iraq in the '*Desert Storm*' campaign, which by their nature could only be indiscriminately directed against geographical areas rather than a specific target, or a means of attack, such as setting a fire in an urban area to force enemy personnel into the open, but which cannot be controlled and is likely to spread indiscriminately affecting civilians and their property along with the intended target.[25]

Fifthly, certain objects such as dams, dykes and nuclear power plants capable of 'releasing dangerous forces' if struck, may only be targeted if they are directly converted into a military function and provide significant support to military operations and no other option is available.[26] The targeting of cultural property is likewise prohibited, except in similar cases and the targeting of objects vital to the survival of the civilian population, or which would cause long-term, widespread and significant harm to the natural environment is prohibited.[27]

Sixthly, weapons or methods of combat which would cause superfluous injury or suffering to enemy combatants are subject to either (far-going) restrictions or are completely banned. The former category includes, inter alia, incendiary weapons and certain types of mines, while the latter includes certain types of munitions (e.g. expanding or flattening bullets) and poisoned, chemical and biological weapons.[28]

---

tionate attacks upon military objectives resulting in excessive (which is not always synonymous with extensive and vice versa) civilian casualties or collateral damage to civilian objects are treated as grave breaches of AP I and constitute war crimes under art 8:2 lit. b (i) and (ii) and (iv) respectively of the Rome Statute of the International Criminal Court.

[24] AP I (n 14) art 57. For the standard of the reasonable commander/combatant, see, inter alia, the Tallinn Manual (n 1) para 13 of the commentary to rule 51 at 163, (rule 113 T.2.0) citing the ruling of the ICTY in the *Prosecutor v Stanislav Galic* (Judgement) [2003] IT-98-29 T para 58.

[25] AP I (n 14) art 51:4, lit. a, b and c respectively.

[26] Ibid., art 56.

[27] Ibid., arts 53, 54 and 55.

[28] Hague Regulations on Land Warfare 1907 art 23(e); ibid., art 35 and specific conventions regulating or banning certain weapons.

Finally, attacks of a perfidious nature (feigning non-combatant or protected status while engaging in attack) are prohibited.[29]

While this summary is not exhaustive, it covers the most important rules relating to the conduct of attacks. In addition, other rules relating to the conduct of hostilities are relevant, such as the duty to refrain from attacks upon protected persons (such as medical personnel) or persons who are *hors de combat* (the wounded, sick, shipwrecked and aircrew bailing out of a stricken aircraft, or who have surrendered at discretion and laid down their arms), so long as they refrain from any hostile act, and the prohibition of denying quarter (not accepting surrender when it is offered or conducting hostilities in a way to allow for no survivors).[30]

4. APPLYING PROPORTIONALITY IN ATTACKS WHICH EMPLOY CYBER WEAPONS

If cyber means and methods of warfare were employed in conducting attacks within the context of an armed conflict, to what extent and how would the law relating to the conduct of attacks set out in the previous section, in particular, the application of the principle of proportionality as it is understood within IHL/LOAC, be relevant? In attempting to answer this question, one should bear in mind a number of considerations. The position taken in the Tallinn Manual and in a number of other publications is that only cyber acts which result in (or are intended to result in) the direct or reasonably foreseeable causation of physical damage, destruction, injury or death are 'attacks' within the context of the law of armed conflict.[31] Consequently, any military operation which does not result in these effects or is intended or reasonably likely to result in such effects (an unsuccessful attack is still an attack), does not involve the principle of proportionality, or any of the other IHL/LOAC rules related to the conduct of attacks. Hence, most military 'information operations', such as psychological warfare, military deception operations designed to mislead the opponent, electronic warfare aimed at jamming or neutralizing electronic communications and weapons guidance or target acquisition systems (unless this was a part of an attack), would fall outside the ambit of 'attack', since they rarely cause such physical effects upon either persons or objects. Likewise the mere gathering of intelligence or conducting of counter-intelligence operations to protect one's own communications and systems, would rarely, if ever, qualify as an 'attack' within the context of the law of armed conflict.[32] That is not to say that there are no relevant rules within IHL/LOAC relating to such operations, but only that these are not related to proportionality and the other rules governing attacks.[33]

---

[29] AP I (n 14) art 37.

[30] First Geneva Convention of 1949 art 24; AP I (n 14) arts 41, 42 and 40 respectively.

[31] Tallinn Manual (n 1) rule 30, with accompanying commentary (rule 92 T.2.0); AP I (n 14) art 49.

[32] For a description and legal analysis of 'information and influence operations', see Blaise Cathcart, 'Legal dimensions of special operations and information operations' in Terry D Gill and Dieter Fleck (eds), *The Handbook of the International Law of Military Operations* (OUP 2015) 449 et seq.

[33] Examples of rules and principles of IHL/LOAC which are not directly related to the conduct of attacks include (but are not limited to) those relating to ruses of war, espionage, misuse of protected, neutral or enemy indicators or status and the duty to take passive precautions (avoidance of locating military objectives in the immediate vicinity of civilians and civilian objects to the maximum extent

Secondly and related to the first point, any operation which only results or is intended to result in mere inconvenience without any foreseeable chance of physical harm or damage, even if this effects the civilian population, equally falls outside the notion of attack, and is not governed by the principle of proportionality. There are two reasons for this: first, because 'attacks' are defined as 'acts of violence' under IHL; and secondly, because proportionality relates to expected collateral civilian death, injury, damage or destruction, which is excessive in relation to the anticipated military advantage from the attack upon a military objective. So if cyber operations resulted in temporary or more prolonged interference with civilian data systems (say e-mail communications or financial transactions), without causing or being intended or likely to cause physical harm (including loss of functionality of the system itself), they would not likely qualify as attacks and proportionality would not be applicable, even if they caused a significant degree of inconvenience and affected daily life to an appreciable extent. Although 'acts of violence' are not limited to the release of physical energy (e.g. chemical weapons are not 'kinetic', but an attack with chemical weapons unquestionably qualifies as an 'attack'), the position taken in the Tallinn Manual is that there must be some physical effects involving damage to, or destruction of, objects, or death or injury of persons for the operation to qualify as an attack, which would make proportionality potentially relevant, and inconvenience, even relatively serious inconvenience, does not normally meet this threshold.[34] On the basis of this interpretation , even if such operations resulted in the destruction or loss of data contained on such systems without resulting in physical harm to persons or damage to objects and without affecting the functionality of the system itself, it would not qualify as an attack in most cases, since data in and of itself has no physical properties.[35] It is arguable, that if the consequences of such destruction of data were reasonably severe, that this could qualify as an act of violence, although this is probably not binding law at present.[36] Moreover if an act were designed to, or likely to result in, the spread of terror or severe mental anguish amongst the civilian population it would, in any case, be prohibited under IHL/LOAC, even if it is not directly related to the notion of proportionality and does not necessarily have any relationship to whether or not data is damaged or destroyed.[37] The destruction of data which could or would likely result in physical effects (e.g. destruction or damage to electronic medical records of patients in a hospital, or the shutdown of a SCADA system controlling a public utility) would in any case qualify as an attack, and depending upon whether it was a side effect of an attack upon a military objective, or simply a deliberate attack upon a civilian system as such, proportionality could enter into the equation. If it were a (foreseeable or unintended) side effect of an attack upon a military objective, proportionality would be relevant and the lawfulness of

---

feasible). These are dealt with in the abovementioned Tallinn Manual (n 1) in the cyber context in rules 59 and 61–66 with accompanying commentary (rules 121 and 123-127 and rule 89 in T.2.0).

[34] Tallinn Manual (n 1) rule 30, para 12 commentary.

[35] The Group of Experts in the Tallinn Manual ibid. unanimously agreed that whenever an attack directed against data resulted in physical harm or destruction above a *de minimis* level it would qualify as an attack. If this included (possible) harm to civilians and civilian objects, proportionality would be applicable. The majority also agreed that if the functionality of the targeted system were affected to a significant extent, requiring physical replacement of components it could qualify as an attack. See 108–9 for discussion of these issues.

[36] Ibid., rule 38 para 5 of the commentary thereto.

[37] AP I (n 14) art 51:2. For discussion of this in the cyber context see, Tallinn Manual ibid., para 8 commentary to rules 30 and 36 with accompanying commentaries.

the attack would (partly) depend upon whether the collateral effects were excessive in relation to the expected military advantage. If it were simply a direct attack upon a civilian system as such, proportionality would not be relevant to its legality, since any such attack is *ipso facto* illegal to start with.[38] But the notion of attack under IHL/LOAC would, according to this interpretation, not necessarily apply to destruction of or damage to data which did not result or was not intended to result in physical harm or damage of some kind. This would arguably exclude cyber operations which had or were likely to have potentially far-reaching negative consequences for the civilian population (without necessarily resulting in physical harm or damage) from the rules regulating the conduct of attacks, including the principles of distinction and proportionality and the taking of feasible precautions to prevent or mitigate harmful consequences to civilians and civilian life. So, for example, a cyber operation which erased registration of vital statistics such as birth, marriage or death, destroyed property records, permanently rendered bank accounts inaccessible or made it impossible for persons to prove their identity would all be potentially excluded from the rules relating to attack according to this interpretation since none of these would likely result in reasonably foreseeable physical harm, no 'violence' is used in simply erasing data or making it inaccessible and data itself is not an 'object' in the literal sense of Article 49 API. These potentially far-reaching negative consequences have resulted in a number of alternative approaches to the question as to when a cyber operation with potentially harmful non-physical consequences could nevertheless constitute an 'attack' which would render the rules relating to the conduct of attacks applicable. These range from treating data as an 'object' to applying the principle of distinction to military operations with more than negligible, transient or easily reversible negative consequences for individual civilians and the civilian population.[39]

---

[38] See section 3 *supra.*

[39] An early example of the view that an operation directed against civilians constituted an attack was put forward by Knut Dörmann in his paper published in 2004 Applicability of the Additional Protocols to Computer Network Attacks' available at https://www.icrc.org/en/doc/assets/files/other/applicability ofihltocna.pdf. Various authors have proposed taking a teleological approach to art. 49. For example, Heather Harrison Dinniss argues in *Cyber Warfare and the Laws of War* (CUP 2012) 179 *ff*, that while data is not itself an object the information systems on which it is located are and that this would result in cyber operations directed against them constituting an 'attack'; Kubo Macak, 'Military objectives 2.0: The case for interpreting computer data as objects under international humanitarian law' (2015) 48 *Israel Law Review* 55 goes further and argues that data should be treated as an 'object' subjecting all actions directed against it to the targeting rules in IHL. The US (DoD) Law of War Manual seems to take an intermediate position by stating that while attacks involve, in principle, a violent act, harmful consequences above the level of temporary or reversible effects, psychological or information warfare or mere inconvenience could constitute an attack to which distinction and proportionality would apply. See DoD Manual (n 16) Chapter 16, Rules 16.5–16.5.2, 1020–22. In view of the disparity in the views of both States and experts and the lack of conclusive evidence of one position or the other constituting a binding interpretation, it seems fair to say that the issue is at present unresolved. My personal view is close to that put forward in the DoD Manual. I believe that the principle of distinction applies to military operations of any kind with potentially harmful consequences for the civilian population that are more than inconsequential or transient which would make a deliberate CNA on a data system such as those set out in the examples in the text above (vital statistics, property records etc.) an indiscriminate attack which is prohibited under IHL/LOAC. To the extent non-physical harmful effects resulted to civilian data (systems) from an attack on a legitimate military objective, the rules relating to proportionality and precautions in conducting attacks would apply since the consequences result from the attack.

Thirdly, any attack not reasonably likely to cause any harm to or appreciable effects upon civilians or civilian objects falls outside the ambit of proportionality even if it causes or results in extensive damage to military objectives or death or injury to persons subject to attack.[40] Hence, an attack upon a self-contained military data system, such as an insulated military communications, target acquisition, or weapons guidance system, as presumably was the case in relation to the earlier mentioned Israeli attack on the Syrian air defence system in 2007, would not involve any considerations of proportionality, since such systems are normally (highly) insulated from civilian systems and little or no question of likely collateral effects arises. Likewise, if the cyber weapon or technique used in an attack were specifically designed to effect only (certain features of) a specific military target and any collateral effects were likely to only be negligible, proportionality would only enter into the equation if the effects turned out to be appreciable and could have been reasonably foreseen. For example, the Stuxnet virus, although used outside the context of an armed conflict, was such a weapon. Although it apparently subsequently spread to a considerable number of (civilian) computer systems in the region, its effects upon them were virtually non-existent or negligible, since it had been specifically designed to only affect certain components within the Iranian nuclear programme.[41] Had it been used within the context of an armed conflict, the question of its proportionality would scarcely, if at all, have been relevant.

Finally, to the extent an attack upon a military objective were (partially) conducted by cyber means, the rules and principles governing attacks would be relevant to the extent the target had a dual use function, or there was an appreciable chance of collateral effects which would meet the threshold of physical damage or personal injury to civilians or civilian objects. This is perhaps stating the obvious, but there can be no doubt that the principle of proportionality would then apply. This would be the case, irrespective of whether the attack were conducted in conjunction with traditional 'kinetic' weapons, or by cyber means alone. In the former case, the principle would apply to all aspects of the attack, including the cyber component thereof, since an attack has to be viewed as a single act and not chopped into separate segments (e.g. loading, aiming and firing a weapon is all part of a single act once it has been completed.) Hence an attack upon a military objective carried out by a combination of cyber and kinetic means should be assessed as a whole.[42] In the latter case involving a stand-alone cyber attack, proportionality would be applicable whenever and to the extent such an attack on a legitimate target was reasonably likely to result in foreseeable collateral physical effects to civilians and civilian objects including damage or destruction of civilian data systems which could result in physical harm or damage. In principle, there is no difference in terms of assessing the legality of such an attack in terms of proportionality from one which was conducted by traditional kinetic weapons. Consequently, it would be lawful to the extent it did not transgress any of the rules relating to the conduct of attacks, including the principle of proportionality. In short

---

[40] See n 22 and accompanying text *supra.*

[41] Rid (n 2) 84–6. It is likely that in both cases, the cyber weapon (virus, worm, etc) was inserted into the targeted systems (which were hardly likely to be connected to the Internet) by means of a removable drive such as a USB stick.

[42] An attack is seen as commencing once a person or object is endangered (e.g. laying a mine is part of an attack long before its detonation). By analogy, a cyber attack commences once malware is introduced which is reasonably likely to result in physical harm or destruction, even if the effect is delayed or fails to occur, due to detection or malfunction. See Tallinn Manual (n 1) paras 14–9 of the commentary to rule 30 (rule 92 T.2.0).

it would be disproportionate if the collateral effects, whether intended or simply a reasonably foreseeable by-product of the attack, were excessive in relation to the anticipated military advantage, based upon the information reasonably available at the time the attack was being planned and conducted. Moreover, it would also depend upon whether all feasible precautions had been taken before and throughout the attack to limit the effects thereof to the maximum extent possible, and where the situation called for it, the attack had been cancelled or suspended once it was in progress if the situation demanded this. Finally, it could also depend upon whether prior warning had been given to civilians before the attack was undertaken whenever this was possible. Examples of such attacks involving cyber weapons or techniques (either alone or alongside traditional weapons) would be against industrial installations, dual-use objects, such as power plants, or communications systems used for both military and civilian purposes. Provided these rose to the level of an attack as set out above, proportionality would govern such attacks in the same way it governs traditional attacks. There are few, if any differences in this regard.

Nevertheless, as stated in the opening sections of this chapter, there is probably little likelihood of such attacks being conducted by purely cyber means alone, aside from exceptional circumstances, for the reasons stated earlier. Consequently, the assessment of proportionality, will in most cases, likely be no different than if the attack had been wholly conducted by kinetic weapons. In any case, the law is the same irrespective of the (combination of) weapons employed.

5. CONCLUDING REMARKS

The main questions posed in the preceding sections of this chapter were to what extent would attacks within the context of an armed conflict which were conducted by digital means, either on their own, or in conjunction with traditional kinetic force, be likely to qualify as 'attacks' under IHL/LOAC (acts of violence resulting in physical harm to persons or damage to objects) and when and to what extent would this involve the applicability of the rules of IHL/LOAC governing the conduct of attacks, including in particular the principle of proportionality *in bello*? On the basis of the preceding examination and discussion of these questions a number of conclusions can be drawn.

First, IHL/LOAC only applies in the context of an armed conflict and no cyber attack on its own has hitherto qualified as reaching the threshold of an armed conflict. However, on at least one occasion (Israel's attack on a Syrian nuclear facility in 2007), cyber means of warfare were reportedly used in conjunction with kinetic force and this without doubt qualified as an attack which was governed by IHL. Moreover any act which caused or was intended to or was reasonably likely to cause any appreciable danger of physical harm or damage would qualify as an attack, if it were carried out within the context of an armed conflict. This could include attacks conducted by digital means, provided the threshold of an armed conflict had been met and the act fitted into the above-mentioned definition and qualification of an 'attack'.

In that context, it was argued that the most likely scenario in which cyber operations would be used as a means of attack would be in conjunction with traditional kinetic weapons as in the example referred to above and that this is more probable within the context of an international armed conflict than in most armed conflicts of a non-international character. This was primarily because most armed groups have neither the capability of mounting a purely

digital operation qualifying as an attack, nor do most of them have the types of sophisticated command, communications and weapons systems which would be the most likely objects of a digital attack. Moreover, many cyber operations which are likely to be engaged in any kind of armed conflict, such as information operations, surveillance and (counter) intelligence do not qualify as attacks and are not subject to the rules governing attack, including the principle of proportionality. Be that as it may, any act which did amount to an attack would nevertheless be governed by the IHL/LOAC rules regulating attacks, if an armed conflict were in progress, irrespective of whether it was of an international or non-international character.

After setting out the applicable law relating to the conduct of attacks, it was further argued that in view of the above-mentioned considerations, seen in context with the function and purpose of the principle of proportionality, as it applies within IHL/LOAC, that only attacks upon military objectives, whereby it was foreseeable that civilians or civilian objects would be affected, would be governed by the principle of proportionality. Hence attacks upon purely military targets, without any likely appreciable consequences to civilians or civilian objects would fall outside the applicability of proportionality. Likewise in any attack which was directed against purely civilian objects or the civilian population, as such, would be *ipso facto* illegal and no considerations of proportionality would enter into assessing its illegality. Consequently, cyber attacks (either on their own or in conjunction with more traditional weapons) upon insulated military systems and similar military objectives, whereby the possible consequences to civilians or civilian objects were non-existent or negligible and attacks upon civilians and civilian objects, as such, are not subject to proportionality considerations.

This still leaves a fairly wide scope for the applicability of the principle of proportionality to attacks in which cyber weapons or techniques could be used. While, as was discussed, there are some specific considerations relating to how the principle would be applied if cyber entered the equation (such as whether destruction of data effecting the civilian population or whether cyber operations with no physical consequences, but resulting in significant harmful effects on the civilian population qualify as 'attacks' in the context of IHL/LOAC), the principle itself and its basic function along with the conditions relating to whether an attack is carried out in conformity with the principle of proportionality, are not significantly, if at all, different when cyber weapons are employed than if they are not. Hence, proportionality applies in much the same way to cyber attacks conducted within the scope of an armed conflict as to any other type of attack, using any weapon, traditional, or non-traditional.

22. Cyber war and the law of neutrality

David Turns[1]

1. INTRODUCTION

The phenomenon of neutrality has been in existence as long as organised warfare itself has characterised less than friendly relations between different peoples, princes and polities. Defined in its most basic sense, in relation to armed conflicts, as the status of non-participation either in a given conflict (temporary neutrality) or in all conflicts (permanent neutrality) with consequent legal rights and duties, it has fulfilled the historically vital function in international relations of legally regulating the co-existence of political entities that are at peace with those that are at war. The legal rights and duties that flow from the status of neutrality attach to both belligerent and neutral powers, and their violation by either party was traditionally seen as a very serious matter since it could entail, among other things, the entry of a previously neutral power into a war and the obligation of the relevant power to make reparations for such violation according to the general international law doctrine of State responsibility. The importance of neutrality during the Age of Exploration (from the fifteenth to the seventeenth centuries) and the subsequent rise of the Nation-State in the post-Westphalian paradigm is not difficult to appreciate: on the one hand, the great European colonial empires with the foundations of their wealth dependent on maritime commerce had a vested interest (as non-belligerents) in ensuring that their merchant shipping would not be unduly caught up in hostile operations during other nations' conflicts and (as belligerents) in enforcing the rules of maritime neutrality to their own advantage and to their enemies' detriment; on the other hand, smaller neutral nations generally saw the economic opportunities for enhanced trade in wartime commodities with belligerents – particularly where the latter were subject to blockade.[2] Meanwhile, all States jealously guarded their territorial sovereignty against infringement by any other States, whether belligerent or not. Classic violations of territorial sovereignty in the context of neutrality consist of such incidents as the boarding and/or capture by a belligerent of an enemy ship at anchor in a neutral port – for example, the capture of the Confederate Navy cruiser *CSS Florida* by the *USS Wachusett* in the harbour at Bahia in flagrant violation of Brazilian neutrality during the American Civil War,[3] and the boarding by *HMS Cossack* of the German oil tanker and supply ship *Altmark* in Jøssingfjord, at a stage in World War II when Norway was

[1] This chapter originates in a paper delivered at a Symposium on the Legal Aspects of Cyber Warfare, held at the Swedish National Defence College in December 2012. All opinions stated herein are those of the author and do not necessarily represent those of the Government, Ministry of Defence or Armed Forces of the UK.

[2] For a useful general discussion of historical attitudes to neutrality in the specific context of naval warfare, see Carl J Kulsrud, *Maritime Neutrality to 1780: A History of the Main Principles Governing Neutrality and Belligerency to 1780* (Little, Brown and Company 1936).

[3] See 'Report of Lieutenant Morris, C.S. Navy, late commanding C.S.S. Florida, of the seizure of that vessel by the U.S.S. Wachusett, October 7, 1864 Bahia, Brazil' in *Official Records of the Union and Confederate Navies in the War of the Rebellion* (Series 1, vol 3, Government Printing Office 1896)

still neutral.[4] Other issues included the impressment of neutral sailors into the naval service of belligerent powers, such as the British practice, during the Napoleonic Wars, of boarding American-flagged ships and forcing American seamen who were alleged to be British subjects or deserters into Royal Navy service.[5] Each such incident was a *cause célèbre* of its day, with important diplomatic and political, as well as legal, repercussions.

As one of the oldest aspects of public international law relevant to the fundamental status of war and peace in international relations, the customary international law of neutrality was largely agreed by the eighteenth century before undergoing progressive codification – in line with other aspects of the laws of war – as part of the Hague Peace Conferences at the beginning of the twentieth century. Although its application was generally considered to be of great practical importance during both World Wars, as in previous wars down the ages, State practice since the adoption in 1945 of the United Nations Charter, with its provisions outlawing the use of force and requiring the co-operation of all Member States with collective security enforcement action mandated by the Security Council, has led to a general tendency to dismiss the laws of neutrality as either at best extant in theory but largely non-applicable in modern practice, or at worst as entirely obsolescent.[6] In the delightful phrase of one commentator, 'They [the rules of neutrality] have a slightly musty quality to them.'[7] With this background to the body of rules under consideration, one may be forgiven for wondering how they can possibly be relevant to the future of armed conflict, and specifically to conflict in cyberspace. On the face of it, neutrality law's traditional obsession with protecting the territorial sovereignty of neutral States seems completely irrelevant in relation to a domain which by definition knows no such concept as either territory or sovereignty. Moreover, in light of the fact that there is as yet no *lex specialis* in international law to govern situations arising in cyberspace, the two topics might appear on the face of it to be mutually incompatible.

This chapter will suggest that such is not necessarily the case, despite the fact that to date there have been no explicit invocations of neutrality law in respect of any international[8] cyber conflict. While the existence of neutrality is a matter of fact based on States' attitudes to a given conflict, the ever-growing interdependence of the world community, not least in eco-

631–3; note the references to Brazilian neutrality in Enclosure 2 (letter of protest from Lt Morris to the President of the Province of Bahia), 634–5.

4 See Brian Simpson, 'The rule of law in international affairs' (2004) 125 *Proceedings of the British Academy* 211, 213–15; Hansard HC Debs vol 357 cols 1161–1164 (20 February 1940); Hansard HL Debs vol 115 cols 576–80 (20 February 1940); 'Correspondence between His Majesty's Government in the United Kingdom and the Norwegian Government respecting the German Steamer "Altmark"' (Cmd 8012, 1950) *House of Commons Sessional Papers, Norway No. 1* vol XXV 451–66.

5 See Walter R Borneman, *1812: The War That Forged a Nation* (HarperCollins 2005) 19–25.

6 As will be argued in this chapter, this conclusion is both exaggerated and premature. It is beyond the scope of this chapter to consider in detail the implications of the adoption of the UN Charter for neutrality law generally, but for a useful discussion, see Detlev F Vagts, 'The traditional legal concept of neutrality in a changing environment' (1998) 14 *American University Intl L Rev* 83, 88–91.

7 Ibid., 84.

8 Although history shows that the laws of neutrality have occasionally been deemed relevant in certain non-international armed conflicts that have had important international implications (principally in cases where each of the contending parties is seen as having some degree of international legitimacy and personality or where the geographical scope of the conflict is such that it has effects outside the territory where the conflict is taking place, the main examples being the American and Spanish Civil Wars), doctrinally it has always been the case that the rules of neutrality are applicable only in conflicts between States.

nomic terms, seems to confirm that 'neutrals cannot simply ignore a war conducted by other countries. "The very nature of war causes its effects to extend also to non-participating States and their nationals, whether they wish it or not."'[9] The chapter will first provide a general overview of the definition, sources and substance of the law of neutrality, before considering how it might apply to conflicts in cyberspace, in terms of both the *jus ad bellum* and the *jus in bello*. Some concluding remarks will indicate the author's views of the possible future for the rules of neutrality in an age of actual or potential cyber conflict.

2. THE INTERNATIONAL LAW OF NEUTRALITY: GENERALITIES

(a) Definition

Neutrality traditionally has two broad meanings, depending on whether it is being discussed in the context of normal peacetime relations or in that of war, i.e., armed conflict; however, it is true to say that as a status it is essentially predicated on the existence of international armed conflict, since that is the only situation in which its legal rules are relevant and operative. In essence, '[n]eutrality (derived from the Latin *neuter* = neither of each) is defined in international law as the status of a State which is not participating in an armed conflict between other States'.[10]

States may adopt a position of permanent neutrality, which is not affected by the temporal existence of any particular armed conflict and is a matter of legal obligation, either voluntarily undertaken by the State in question as a matter of its domestic law[11] or imposed on it by international treaty.[12] Probably the most famous example of a permanently neutral State is Switzerland, whose self-described tradition of 'reticence in foreign policy' dates back to at least 1515, was formally recognised by the Great Powers of Europe at the Congress of Vienna in 1815 and has been incorporated into successive Federal Constitutions since 1848.[13] More recent examples include the acceptance of permanently neutral status by Austria in 1955 – despite the adoption of a national constitutional law which gave the appearance of voluntary adoption, it had actually been a pre-requisite for the withdrawal of post-World War II Soviet occupation forces and ratification of the Austrian State Treaty, and had therefore been agreed

---

[9] Yoram Dinstein, *War, Aggression and Self-Defence* (CUP 2005) 24–5 (citing Eric Castrén, *The Present Laws of War and Neutrality* (Suomalainev Tiedeakemia 1954)).

[10] Dieter Fleck (ed), *The Handbook of International Humanitarian Law* (OUP 2013) § 1101.

[11] During the interwar period the US Congress adopted domestic legislation establishing US neutrality as a matter of domestic legal obligation: see US Department of State, Office of the Historian, 'The Neutrality Acts, 1930s' http://history.state.gov/milestones/1921-1936/neutrality-acts.

[12] One of the most famous historical examples of permanent neutrality being imposed on a sovereign State by international agreement was Belgium, under the Treaty of London (1839). It was the violation of this treaty by Germany in 1914 that was the immediate cause of Great Britain's involvement in the First World War. The Vatican City State also agreed to permanent neutrality under art 24 of the Treaty of Conciliation, part of the 1929 Lateran Pacts with Italy, as a condition of continued papal independence following Italian unification.

[13] Swiss Federal Department of Defence, Civil Protection and Sports, *Swiss Neutrality* (4th edn) 4–10 http://www.vbs.admin.ch/internet/vbs/en/home/documentation/publication.parsys.0008.downloadList.9934.DownloadFile.tmp/neuteebook.pdf.

in advance by the former Allied Powers[14] – and the UN General Assembly's recognition of Turkmenistan's permanent neutrality, as provided for in its national legislation.[15] It is also possible for a designated part of the territory of a State to be permanently neutral, as opposed to the State as such.[16] Permanent neutrality as a status under public international law is not to be confused with either *de facto* neutrality[17] or a *policy* of neutrality. The latter – as practiced by Sweden through most of the nineteenth and twentieth centuries, Ireland since 1937 and Finland during the Cold War – is characterised by the absence of any legal obligation; as a unilateral policy decision of the relevant government, it may of course be changed very rapidly and does not necessarily entail international recognition.

In practice very few States have ever been, or are today, permanently neutral in the legal sense. By far the more common usage of the term 'neutrality' is in relation to what is effectively temporary neutrality, which in international law is defined as being the position of any State that does not participate in armed hostilities between two or more other States;[18] this is in fact automatically the *de jure* status of such non-participating States. As such, temporary neutrality has no legal application outside international armed conflicts and requires no formal declaration or explicit acknowledgment: its existence is entirely dependent on there being a factual situation of armed conflict.[19] It entails very specific rights and duties in the relationship between neutral and belligerent States, which arise as a matter of legal obligation under international law. Being so fact-dependent, it is logical that the laws of neutrality apply only so long as a conflict lasts, and in relation to any particular State may be further limited by that State's attitude to the conflict in question. A State may adopt a position of neutrality at the outset of a conflict, only to find itself embroiled therein as a belligerent at a later point in time through hostile action or occupation by one or more belligerents, as in the cases of Denmark, the Netherlands and Belgium during World War II, following their 1940 invasion by Germany. Similarly, a belligerent State may withdraw from a conflict and assume the position of a neutral, as in the case of Russia in World War I, following the 1918 Treaty of Brest-Litovsk with the Central Powers. Finally, although it is relatively unusual, a State may be a belligerent vis-à-vis certain States but neutral vis-à-vis others that are allied to those belligerents: during World War II for example, although the Soviet Union was at war with

---

[14] *Bundesverfassungsgesetz vom 26. Oktober 1955 über die Neutralität Österreichs*, *Bundesgesetzblatt für die Republik Österreich* Nr. 211/1955.

[15] UNGA Res A/50/80 [A] (11 January 1996) UN Doc A/RES/50/80.

[16] E.g., the Panama Canal Zone, under art XVIII of the Hay-Bunau-Varilla Treaty (Convention for the Construction of a Ship Canal, 18 November 1903 http://avalon.law.yale.edu/20th_century/pan001.asp) was declared 'neutral in perpetuity'; the first of the Corrijos-Carter Treaties confirmed this status (Treaty Concerning the Permanent Neutrality and Operation of the Panama Canal (7 September 1977) arts 1–2 http://www.pancanal.com/eng/legal/neutrality-treaty.pdf.

[17] Primarily this would result from a State's voluntary abolition of its own armed forces: examples are Liechtenstein (since 1868) and Costa Rica (since 1949). On the other hand, Iceland has voluntarily had no armed forces since achieving independence from Denmark in 1944, but is a member of the North Atlantic Treaty Organisation and is thus considered a neutral State neither *de jure* nor *de facto*.

[18] Fleck (n 10).

[19] At customary international law the generic definition of armed conflict has been expressed as existing, 'whenever there is resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State': *Prosecutor v Dusko Tadić* (*Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction*) [1995] No ICTY-94-1-A para 70.

Germany and Italy in the European theatre of the war from 1941, legally it remained neutral and at peace in respect of the third Axis Power, Japan, right up until the last three weeks of hostilities in the Pacific theatre in 1945.

Temporary neutrality in turn is not to be confused with *non-belligerency*, which is the practice certain States have adopted, in specific conflicts, of providing assistance to one or other of the belligerent parties without becoming directly involved in armed hostilities; classic examples (all in the context of World War II) include American economic support and provision of war materiel to Britain under the Lend-Lease Program[20] before America's entry into the war in December 1941, the very extensive and wide-ranging forms of practical assistance provided by Ireland to the UK and US throughout the war (or rather, 'the Emergency' – the somewhat Orwellian term coined by the Irish Government to characterise Ireland's position of 'friendly neutrality' vis-à-vis the Allied Powers),[21] and the Spanish provision of volunteer troops – the famous Blue Division – to fight with the German and other Axis forces, under German overall command and control, against the Soviet Union on the Eastern Front.

(b) Sources

In common with much of the modern law relevant to armed conflict, the rules of neutrality had their origin in customary international law developed over many centuries before undergoing a process of codification at the beginning of the twentieth century. In addition to a substantial body of national judicial decisions, many of them by British and American courts and relating mostly (though not exclusively) to the application of neutrality rules in warfare at sea,[22] the contemporary law of neutrality is mainly to be found in two treaties that emerged from the Second International Peace Conference held at The Hague in 1907, along with one earlier document from the conclusion of the Crimean War (1853–56). The Paris Declaration Respecting Maritime Law of 16 April 1856[23] purported to abolish the ancient practice of privateering and assure the protection of neutral ships and goods at sea; in 1907, detailed rules regulating the presence and activities of belligerent warships in neutral ports and territorial waters were laid down in the Hague Convention (XIII) concerning the Rights and Duties of Neutral Powers in Naval War.[24] Extensive equivalent rules for the land domain in hostilities were stipulated in the Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land[25] and have also in recent years been restated with considerably more modern language and concepts – albeit not in the internationally binding form of a treaty – for

---

[20] An Act to Further Promote the Defense of the United States (Pub L 77–11, H.R. 1776, 55 Stat. 3034, enacted March 11, 1941).

[21] See Mervyn O'Driscoll, 'Keeping Britain sweet: Irish wartime neutrality, political identity and collective memory' in E Grollet, *Collective Memory in Ireland and Russia: Conference Proceedings* (Rosspen 2007).

[22] For examples, see Leslie C Green, *The Contemporary Law of Armed Conflict* (Manchester University Press 2008) 302–4.

[23] Declaration Respecting Maritime Law (16 April 1856) British State Papers 1856 vol LXI 155.

[24] (1908) 2 AJIL Supp 202.

[25] (1908) 2 AJIL Supp 117.

both the maritime[26] and air[27] domains of warfare. Notwithstanding the relative antiquity of the Hague Conventions V and XIII, it was already generally considered at the time of their adoption that they were declaratory of customary international law;[28] that being the case, and as they remain in force for the State parties,[29] their provisions would be of general applicability in the event of neutrality law being invoked in an international armed conflict today. Some of the other Hague Conventions adopted in 1907 also touch on the subject of neutrality, namely Convention (VIII) Relative to the Laying of Automatic Submarine Contact Mines[30] and Convention (XI) Relative to Certain Restrictions with Regard to the Exercise of the Right of Capture in Naval War,[31] and certain relevant rules are also restated in the military manuals of various States,[32] thereby providing further evidence of their customary law status.

With the exception of the modern restatements mentioned – which are not treaties as such anyway and of which only the Harvard Manual can really be said to belong to the cyber age – it will be noted that the treaty instruments and the customary rules which they largely codify are of considerable antiquity; they pre-date even the invention of computers, let alone the concept of cyber warfare. It has become something of a truism to make the point that there is no *lex specialis* in international law specifically governing activities in cyberspace: the treaties are too old, and State practice – what little of it that may have been identified to date – is so fragmented and inconsistent that it is difficult to speak of customary *lex lata* in this area.[33] However, there are two international documents that make express reference to neutrality in armed conflict and are applicable, by analogy in the one case and expressly in the other, to cyber war; these are, respectively, the Hague Rules for the Control of Radio in Time of War,[34] and the *Tallinn Manual on the International Law Applicable to Cyber Warfare, Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence*

---

[26] Louise Doswald-Beck (ed), *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* (CUP 1995).

[27] Harvard Program on Humanitarian Policy and Conflict Research, *Manual on International Law Applicable to Air and Missile Warfare* (Harvard University 15 May 2009) Section X Rules 165–75 [Harvard Manual] http://www.ihlresearch.org/amw/manual/. Certain provisions of an earlier unratified instrument had previously addressed aspects of neutrality in respect of the air domain: see The Hague Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare, Part II: Rules of Aerial Warfare (Cmd 2201) *House of Commons Sessional Papers, Miscellaneous no. 14* (1924) vol XXVII 1031–76. Whereas the Hague Rules were neither adopted nor ratified as a treaty although it was originally hoped that they might attain that legal status, the Harvard Manual does not purport to be a treaty at all. Although the legal value of these documents might therefore appear questionable, to the extent that they mirror rules found in the treaties on land and maritime warfare or restate otherwise pre-existing rules, they may be said to represent customary international law.

[28] Adam Roberts and Richard Guelff (eds), *Documents on the Laws of War* (OUP 2000) 85 and 127.

[29] There are 33 State parties to Convention V, and 29 to Convention XIII: see International Committee of the Red Cross, 'Treaties and State Parties to Such Treaties' http://www.icrc.org/ihl.

[30] (1908) 2 AJIL Supp 138.

[31] (1908) 2 AJIL Supp 167.

[32] E.g., Fleck (n 10), which incorporates the 1992 German Joint Services Regulations (ZDv 15/2); UK Ministry of Defence, *The Manual of the Law of Armed Conflict* (OUP 2004); US Department of the Navy et al, *The Commander's Handbook on the Law of Naval Operations*, NWP 1–14M (ed July 2007).

[33] But see below, text accompanying Tallinn Manual (n 35) rule 5.

[34] The Hague Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare, Part I: Rules for the Control of Radio in Time of War (n 27) 1021–30.

Centre of Excellence.[35] Again, a note of caution is necessary as to their normative status: the Hague Rules were never opened for signature and ratification as a binding treaty, while the Tallinn Manual is the work of individuals not purporting to express the official opinions of any States or organisations;[36] technically, therefore, neither document is legally binding per se. In the case of the Hague Rules, it is not entirely clear from the *General Report of the Commission of Jurists to Consider and Report upon the Revision of the Rules of Warfare* precisely which (if any) provisions of the rules in Part I were already considered to be customary international law; in many cases, inevitably in light of the relatively recent development of radio technology at the time, the rules were derived from conventions which themselves were of comparatively recent origin.[37] The Tallinn Manual is arguably going to be of greater normative value since it is grounded in the acknowledged existing law, which it seeks to extend to cyber conflict:

> The International Group of Experts was unanimous in its estimation that both the *jus ad bellum* and *jus in bello* apply to cyber operations. Its task was to determine how such law applied, and to identify any cyber-unique aspects thereof. The Rules set forth in the *Tallinn Manual* accordingly reflect consensus among the Experts as to the applicable *lex lata*, that is, the law currently governing cyber conflict.[38]

Rules 91–95 of the original edition of the Tallinn Manual directly dealt with the issue of neutrality in cyber operations; in the second, and current, edition,[39] the equivalent Rules are numbered 150-154. The substantive provisions and commentaries relating to neutrality are identical as between the two editions of the Tallinn Manual and will be discussed below.

(c) Substance

Without going into every particular of the general laws of neutrality, for present purposes, their essential principles may be said to be the 'two pillars' of non-participation and non-discrimination;[40] the first principle entails specific rights and duties for both neutral and belligerent States, while the second is applicable only in respect of certain actions of neutral States.

Non-participation means that, on the one hand, the territorial sovereignty of a neutral State must not be violated by any belligerents, while on the other hand, a neutral State is not allowed actively to participate in armed hostilities or to allow such participation from its territory. The rule regarding inviolability of territorial sovereignty differs between the land and maritime domains: whereas the land territory of neutral States is absolutely inviolable,[41] the mere presence of belligerent warships in neutral territorial waters is not per se unlawful as

---

[35] Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013) [Tallinn Manual].

[36] Ibid., 9–10.

[37] See The Hague Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare, Part II: Rules of Aerial Warfare (n 27) 1021–22.

[38] Tallinn Manual (n 35) 5.

[39] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) [Tallinn Manual 2.0]. References hereinafter to specific Rules in the Tallinn Manual are to the second edition.

[40] Dinstein (n 9) 24.

[41] HC V, art 1.

long as they abstain from '[a]ny act of hostility',[42] and in the decades since 1907 the general international law of the sea has additionally recognised a right of transit through neutral international straits and archipelagic sea lanes (in addition to the long-standing customary right of 'innocent passage'), which the modern law of armed conflicts at sea expressly preserves.[43] Air operations are correspondingly regulated, according to whether they take place over land or sea:[44] for example, the British dropping of propaganda leaflets over the city of Rome during World War II elicited a diplomatic protest from Pope Pius XII, who considered the fact that some of them fell to earth within the precincts of the Vatican to be a breach of the Holy See's neutrality.[45] While belligerent powers may not violate neutral territory by moving troops or military convoys across,[46] erecting communications installations on,[47] or forming combatant forces in[48] it, neutral powers are themselves under a positive duty not to permit such actions to take place within their territory.[49] The corresponding duty of the neutral State in maritime warfare is inevitably less extensive in view of the permitted presence of belligerent warships in neutral ports and waters, although it does include the special obligation to prevent the fitting out, arming or departure of any vessel intended for hostile operations.[50]

While it is self-evident that neutral States must not participate in hostilities, their duty of non-discrimination is perhaps less well-known; it requires such States to apply with complete impartiality, as between the belligerents, certain specific restrictions and prohibitions. For example, 'the conditions, restrictions, or prohibitions made by [a neutral power] in regard to the admission into its ports, roadsteads, or territorial waters, of belligerent war-ships [*sic*] or of their prizes' must be applied impartially to both sides in a conflict at sea.[51] Although by the time of World War II it was generally understood that the internment of belligerent aircraft and their aircrews shot or forced down over any neutral State's airspace was to be applied impartially,[52] the Irish practice of instructing Allied aircrew to report that their flight was on non-combatant duty (so that they could quietly be sent across the border to Northern Ireland) whilst insisting on the internment of all German aircraft and aircrew, became a matter of some notoriety.[53] Such attitudes, as mentioned above, effectively amount to non-belligerency – also

---

[42] HC XIII, arts 1 and 2. Belligerent warships may remain in neutral ports for necessary repair of battle or storm damage; thus, the German pocket battleship *Admiral Graf Spee's* sojourn in Montevideo harbour after the Battle of the River Plate in 1939 fully respected Uruguayan neutrality (see also ibid., arts 12–14).

[43] See Doswald-Beck (n 26) §§ 23–33.

[44] See Harvard Manual (n 27) rules 167(a), 170(a) and 172(a)(ii).

[45] See Owen Chadwick, *Britain and the Vatican During the Second World War* (CUP 1986) 222.

[46] HC V, art 2.

[47] Ibid., art 3. For the equivalent provision in respect of maritime warfare, see HC XIII, art 5.

[48] HC V, art 4.

[49] Ibid., art 5.

[50] HC XIII, art 8. This codified the customary law position that had been argued successfully by the US in its post-Civil War proceedings against Great Britain for the latter's failure to prevent the construction in, and departure from, its ports of Confederate commerce raiders such as the *CSS Alabama* and *CSS Florida*: see John B Moore, *History and Digest of the International Arbitrations to Which the United States Has Been a Party* (vol I, Government Printing Office 1898) ch XIV 495–682 and 653–9; Tom Bingham, 'The Alabama Claims Arbitration' (2005) 54 *Intl and Comparative L Quarterly* 1.

[51] HC XIII, art 9.

[52] See The Hague Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare, Part II: Rules of Aerial Warfare (n 27) art 42, and commentary at 1054–55.

[53] See O'Driscoll (n 21) 12–4.

sometimes referred to as 'qualified neutrality' – but still have in common with strict observance of neutrality the avoidance of active participation in armed hostilities. The same is true of the requirement that neutral States not give assistance to the parties to a conflict: this does not extend to a prohibition on selling 'arms, munitions of war, or, in general … anything which can be of use to an army or a fleet'[54] and the duty of non-discrimination does not mean that such sales must be extended equally to both sides in a conflict,[55] although if a neutral State decides to ban such exports, it must do so on a non-discriminatory basis.

On a more general level, it has long been accepted that neutral States are absolutely entitled to defend their territorial sovereignty against any and all infringements by belligerent forces, but the fact that a State may do so in accordance with the right of self-defence as a matter of the *jus ad bellum* does not turn it into a belligerent and cannot be regarded as a hostile or wrongful act under international law.[56] Conversely, if a neutral State is unwilling or unable to prevent the use of its territory for hostile operations against a belligerent (a failure which comes within the definition of aggression in customary international law),[57] the latter may be entitled to use force in self-defence against hostile forces in the neutral State, subject to the normal rules of the *jus ad bellum*.

Finally, the effect of the advent of the UN Charter regime (as regards the legality of the use of force) on the traditional law of neutrality should be noted. As Vagts has remarked, 'war and neutrality were both thought rendered obsolete by the coming of the United Nations and its regime of collective security. That is not quite accurate'.[58] The Charter undoubtedly has significance for neutrality in that it requires all Member States of the UN, on the one hand, to co-operate with collective security enforcement measures mandated by the Security Council under Chapter VII of the Charter,[59] and on the other hand, to refrain from rendering any assistance to States that are the object of such enforcement measures.[60] The former obligation might suggest that there is no scope for a State to remain neutral *stricto sensu*, once the Security Council has ordered enforcement measures against another State,[61] while the latter obligation could imply the abandonment of impartiality in the provision of any 'arms, munitions of war, or… anything which can be of use to an army or a fleet'.[62] However, State practice since 1945 has indicated that the traditional law of neutrality continues to be invoked by States, Chapter VII of the Charter notwithstanding. The Korean War (1950–53) saw ambivalent stances

---

54 HC V art 7.

55 See below n 62.

56 See HC V art 10; HC XIII art 26.

57 UNGA Res 3314 (XXIX) (14 December 1974) Annex – Definition of Aggression art 3(f). Note, however, that this requires the territory to have been 'placed at the disposal of another State': absent such consent – as, for example, in the case of a failed State or one without an effective government in control of the territory – it is not likely that aggression would be imputed to the neutral State itself.

58 Vagts (n 6) 84.

59 UN Charter arts 2(5), 25 and 49.

60 Ibid., art 2(5).

61 In support of this view, see Christian Lanz, 'Is neutrality an appropriate instrument for domestic security? A European perspective' (2005) 17 *Information and Security* 41–9 and 42–3.

62 HC V, art 7. The requirement to comply with an arms embargo at the direction of the Security Council under art 41 of the Charter, e.g., would negate this obligation for neutral States: see Vagts (n 6) 89.

and contradictory behaviour by several States,[63] not least the People's Republic of China, which steadfastly insisted that it was neutral despite the large-scale combat operations of the 'Chinese People's Volunteers' against the UN forces whose presence in Korea was mandated by Security Council Resolutions 83 and 84.[64] The inconclusiveness of military ground offensives during the Iran-Iraq War (1980–88) led both belligerents to attack neutral shipping in the Persian Gulf in an attempt to interdict each other's oil trade (the so-called 'Tanker War'), which severely impeded the right of neutrals to trade with belligerents;[65] this, coupled with the overtly ambivalent attitude adopted by several non-belligerent States in the conflict[66] gave rise to considerable debate as to the relevance and application of the law of maritime neutrality.[67] The Security Council repeatedly condemned all infringements of neutral States' territorial waters as well as attacks on neutral shipping,[68] which clearly indicated that the rules of neutrality were deemed to be still applicable; the practice adopted by certain neutral States of reflagging their merchant vessels for protection by US and other powerful naval forces – themselves belonging to neutral nations – present in the Persian Gulf, while not completely uncontroversial, was not viewed as subverting neutrality law.[69]

It has been suggested that it was the Security Council's failure to designate an aggressor in the Iran-Iraq War that 'made it possible for other states to assume the status of traditional neutrality';[70] however, subsequent State practice on point is extremely limited. During the subsequent crisis and conflict in the Persian Gulf resulting from the Iraqi invasion of Kuwait (1990–91), the Americans and their Coalition partners accepted a 'modified nature of neutrality' in the situation of enforcement action being taken pursuant to a Security Council mandate:[71] the Jordanian and Iranian proclamations of neutrality were respected, on the understanding that they were 'subordinate to [those nations'] obligation as UN members to

---

[63] E.g., Operation TP Stole, a Central Intelligence Agency-masterminded takeover of a Norwegian ship chartered by the Communist Chinese to take Indian medical supplies to North Korea (Norway and India both proclaimed their neutrality in the Korean War): see Paul M Edwards, *Combat Operations of the Korean War: Ground, Air, Sea, Special and Covert* (McFarland and Co. 2010) 165–6.

[64] UNSC Res 83 'Complaint of aggression upon the Republic of Korea' (27 June 1950) UN Doc S/RES/83; UNSC Res 84 'Complaint of aggression upon the Republic of Korea' (7 July 1950) UN Doc S/RES/84. Chinese military participation in the Korean War was characterised by the General Assembly as aggression: UNGA Res 498(V) (1 February 1951) UN Doc A/RES/498 (V).

[65] See Andrea Gioia and Natalino Ronzitti, 'The law of neutrality: Third states' commercial rights and duties' in Iger F Dekker and Harry G Post, *The Gulf War of 1980–1988: The Iran-Iraq War in International Legal Perspective* (Martinus Nijhoff Publishers 1992) 221–42. Iraq expressed the view that neutral merchant ships trading with Iran forfeited their neutral character: UNSC 'Letter dated 20 February 1985 from the Permanent Representative of Iraq to the United Nations addressed to the Secretary-General' (20 February 1985) UN Doc S/16972 para 2.

[66] E.g., France supplied arms and military equipment to Iraq only, while the US specifically denied arms and war materials to Iran only: Dekker and Post (n 65) 228–9.

[67] See, e.g., Francis V Russo, 'Neutrality at sea in transition: State practice in the Gulf War as emerging customary international law' (1988) 19 *Ocean Development and Intl L* 381; Boleslaw A Boczek, 'Law of warfare at sea and neutrality: Lessons from the Gulf War' (1989) 20 *Ocean Development and Intl L* 239–71.

[68] Ibid., 260.

[69] See Michael H Armacost, 'U.S. policy in the Persian Gulf and Kuwaiti reflagging' (1987) 10 *Defense Institute of Security Assistance Management J* 11, 14; Margaret G Wachenfeld, 'Reflagging Kuwaiti tankers: A U.S. response in the Persian Gulf' (1988) 37 *Duke L J* 174.

[70] Boczek (n 67) 254.

[71] UNSC Res 678 (29 November 1990) UN Doc S/RES/678.

comply with UNSC resolutions'; the US asserted that, 'regardless of assertions of neutrality, all nations were obligated to avoid hindrance of Coalition operations undertaken pursuant to, or in conjunction with, UNSC decisions, and to provide whatever assistance possible'.[72] This extended, in the US interpretation, to a requirement for Iran to return any downed Coalition aircraft and aircrew instead of interning them, as required by Article 5 of Hague Convention V, and to the permissibility of US entry into neutral airspace to rescue such aircraft or aircrew, 'consistent with [US] international obligations as a belligerent'.[73] Further, in respect of neutral States' trade with Iraq, it was the US position that, '[the UNSC] resolutions modified the obligation of neutral powers to remain impartial with regard to Coalition UN members'.[74]

3. THE INTERNATIONAL LAW OF NEUTRALITY IN THE CYBER CONTEXT

(a) Generalities

It has been clear from the outset that any discussion of neutrality law in the context of cyber conflict at this point in time must be highly speculative, to say the least. The normative sources of neutrality law, as briefly discussed above, date from an era when computers and cyber networks had not even been imagined, and their substance is heavily reliant on such tangible constructs as territory, territorial waters and airspace (above both land and the territorial sea). Cyber networks, by their very nature, are intangible and appear unsusceptible per se to any exercise of national jurisdiction or sovereignty. As has been colourfully suggested with reference specifically to maritime neutrality laws, 'their dispositions with regard to naval passage through neutral waters and into neutral ports reflect a world in which sweating teams of stokers moved coal from bunkers to furnaces beneath boilers'.[75] Quite apart from the total lack of clearly accepted *lex scripta* regulating cyber neutrality, there is also an equally total lack of any relevant State practice: as far as is known there have been no purely cyber conflicts to date, and the only armed conflict in which cyber operations were unquestionably conducted within the context of the conflict has not resulted in any legal determination of wrongfulness and/or responsibility for such operations. During the South Ossetia War (2008), both Russian and Georgian media websites were hacked, as well as Georgian official government websites; neutrality was ostensibly implicated, however, insofar as it was alleged that Russian hackers inflicted distributed denials of service (DDOS) on Azerbaijani news websites, while the governments of Estonia and Poland offered technical assistance by hosting Georgian official websites and sending cyber-defence advisers to Georgia.[76] As far as is known, Azerbaijan

---

[72] US Department of Defense, 'Final Report to Congress: Conduct of the Persian Gulf War, Appendix O – The Role of the Law of War' (1992) 31 *Intl Legal Materials* 615, 638. As examples of neutral States' attitudes, Austria and Switzerland both permitted overflights by US military transport aircraft, whereas India did not: ibid. 640.

[73] Ibid., 639.

[74] Ibid., 640.

[75] Vagts (n 6) 84.

[76] See Noah Shachtman, 'Estonia, Google Help "Cyberlocked" Georgia (Updated)', *Wired* (8 November 2008) http://www.wired.com/dangerroom/2008/08/civilge-the-geo/; Stephen W Korns and Joshua E Kastenberg, 'Georgia's cyber left hook' (2008) XXXVIII(4) *Parameters* 60.

never objected to the putative violations of its neutrality, while Estonia and Poland were not condemned for their own violations – if indeed their actions amounted to violations. No State acknowledged responsibility for any hacking or DDOS operations; Russia claimed that the hacking of Georgian websites was undertaken by 'patriotic activists' (or 'hacktivists') spontaneously and outside any governmental control.[77]

Nevertheless, in spite of the difficulties, it is submitted that the law of neutrality can, should, and probably will in due course be applied to cyber conflicts, by interpretative analogy and in light of the objects and purposes of the law – i.e., protection of the interests of neutral and belligerent States alike; a similar extension has previously been foreseen in respect of the use of satellites and other modern communications technology in outer space.[78] Moreover, the references to neutrality in recent manuals and accompanying commentaries – the Harvard and Tallinn Manuals – unofficial and non-normative though their legal status may be, as well as in official national military manuals,[79] clearly indicate that current expert opinion continues to hold a place for neutrals' rights and duties in the modern law regulating resort to and conduct of armed (including cyber) conflict.

(b) Expressly Applicable Rules

As noted in the Tallinn Manual, 'The International Group of Experts unanimously agreed that the law of neutrality applied to cyber operations'.[80] Indeed, the Experts assert that:

> The global distribution of cyber assets and activities, as well as global dependence on cyber infrastructure, means that cyber operations of parties to a conflict can easily affect private or public neutral cyber infrastructure. Accordingly, neutrality is particularly relevant in modern armed conflict.[81]

As will be discussed below, the present author believes that there is at least a 50 per cent probability that this is an accurate assessment of the future for neutrality law in cyber conflict,

---

[77] See John Markoff, 'Before the gunfire, cyberattacks', *The New York Times* (12 August 2008) http://www.nytimes.com/2008/08/13/technology/13cyber.html?emand_r=0; Paulo Shakarian, Jana Shakarian and Andrew Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (Syngress 2013) Ch 3.

[78] See David L Willson, 'An Army view of neutrality in space: Legal options for space negation' (2001) 50 *Air Force L Rev* 175, 192–204.

[79] E.g., Office of General Counsel, US Department of Defense, *Law of War Manual* (June 2015, Updated May 2016) § 16.4; France, Ministère des Armées, *Droit international appliqué aux operations dans le cyberespace* (2019) § 2.3.

[80] Tallinn Manual 2.0 (n 39) Ch 20 para 1.

[81] Ibid., para 3.

notwithstanding the fact that no State has as yet declared neutrality in any cyber conflict. The Tallinn Manual specifies just five rules of *lex lata*[82] in relation to cyber neutrality, namely:

- The prohibition of hostile acts[83] by belligerents against neutral cyber infrastructure;[84]
- The prohibition of belligerent cyber operations using infrastructure within neutral territory;[85]
- The duty of a neutral State not to allow belligerent cyber operations 'from cyber infrastructure located in its territory or under its exclusive control';[86]
- The right of a belligerent to 'take such steps, including by cyber operations, as are necessary' against a neutral State that fails to prevent belligerent operations in accordance with Rule 152;[87] and
- The necessity for neutral States to act in a manner compatible with any collective security enforcement measures ordered by the UN Security Council under Chapter VII of the UN Charter.[88]

Rules 150–152 may be characterised as part of the *jus in bello* and are derived directly from the relevant Hague Conventions of 1907 – respectively, Article 1 of both HC V and HC XIII (Rule 150), Articles 2 and 3 of HC V and Articles 2 and 5 of HC XIII (Rule 151), and Article 5 of HC V (Rule 152). Rules 150 and 151 are basically opposite sides of the same coin in that they prohibit violations of neutrality, whether directed against or emanating from neutral cyber infrastructure. Rule 152 reaffirms the duty of neutral States, where possible, to prevent violations occurring on their territory. These Rules clearly reflect only the 'first pillar' of the traditional law of neutrality: the principle of non-participation. While this principle thus remains the bedrock of a contemporary concept of neutrality, the nature of the modern global economy and international commercial realities, as illustrated by State practice in the Iran-Iraq and First Gulf Wars discussed above, as well as the inherent practical and technical difficulties in the regulation of cyber activity, seem to suggest that the 'second pillar' of non-discrimination may become less important in future applications of neutrality law – in the cyber context as in more conventional armed conflicts.[89]

---

[82] Each of the first three rules is claimed to represent a norm of customary international law, as reflected in the Hague Conventions V and XIII. The fourth, as a form of 'self-help', is said to be 'generally accepted as customary international law' (Tallinn Manual 2.0 (n 39) rule 153, para 1); although little evidence is cited to justify such an assertion, it may be safely assumed that it would fall within the category of self-defence under the *jus ad bellum* (cf. *UK Ministry of Defence* (n 32) para 1.43(a)). The fifth is derived from a treaty, namely the UN Charter, under art 103 of which customary law rules that are incompatible with a rule contained in the Charter are superseded by the latter.

[83] The Experts note that they chose to use the term 'exercise of belligerent rights' as a synonym for 'hostile act' (the principal term which is used in the Hague Conventions); the preference is explained by reference to the latter term being 'an operational term of art', although the point is not elucidated further: Tallinn Manual 2.0 (n 39) Ch 20, para 6. The present author considers the sense of the term 'hostile act' to be clear enough from the context.

[84] Ibid., rule 150.

[85] Ibid., rule 151.

[86] Ibid., rule 152.

[87] Ibid., rule 153.

[88] Ibid., rule 154.

[89] Although note that the duty of non-discrimination is acknowledged in that any restrictions on the use of open, publicly accessible networks (e.g., the Internet) must be 'impartially applied to all parties to

(c) Selected Issues: Jus ad Bellum

Rules 153 and 154 of the Tallinn Manual are concerned with the cyber dimension of neutrality in respect of the two Charter-based exceptions to the prohibition of the use of force in international relations: self-defence (although the Manual does not use that term at this point) and collective security enforcement measures ordered by the Security Council in the exercise of its Chapter VII powers. Indeed, it is arguable that the law of neutrality is of very little relevance to the initiation of cyber conflicts except in these two respects. It is interesting to note, however, that Rule 153 is concerned with *a belligerent's* right to use force, if necessary, to counter cyber violations of a State's neutrality – not with *a neutral State's* right to defend its neutrality by armed force, including cyber operations, if necessary. Perhaps it was assumed by the Experts that the neutral State's right of self-defence in such circumstances would be so self-evident as to render discussion unnecessary. Nevertheless, it bears emphasising that, since every State always has the inherent right to defend its territorial sovereignty and political independence from attack,[90] the Tallinn Manual repeatedly mentions the unlawful use of cyber infrastructure on a neutral State's territory, and the Hague Conventions expressly recognised that a neutral State's use of force in defence of its rights is not to be regarded as a hostile or unfriendly act by the belligerent(s) against which such action is directed,[91] by analogy a neutral State clearly would be permitted to defend its neutrality against cyber violations.

As regards the precise formulation used in Rule 153, it may be noted that it presupposes knowledge by the neutral State of the violation. However, the notorious difficulty of tracing – much less of attributing – cyber activity with any great degree of precision[92] may impose an altogether unreasonable burden on the authorities of a neutral State, even when the principle of due diligence in preventing violations of international law is taken into account.[93] As opined by the International Court of Justice (ICJ) in the very first contentious case ever submitted to it for adjudication:

> it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein, nor yet that it necessarily knew, or should have known, the authors. This fact, by itself and apart from other circumstances, neither involves *prima facie* responsibility nor shifts the burden of proof.[94]

It is submitted that this may *a fortiori* be the case in the cyber context, as in the situation where an agent of a belligerent State briefly enters the territory of a neutral State and, while present there, opens a laptop computer and sends an e-mail containing a virus that infects the military

---

the conflict': ibid. rule 152, para 3. This could apply, for instance, in the context of restricting belligerent Internet traffic from transiting via servers hosted in a neutral State – a measure which would surely be remarkably difficult to enforce.

90 UN Charter art 51.

91 HC V, art 10; HC XIII, art 26.

92 See Nicholas Tsagourias, 'Cyber attacks, self-defence and the problem of attribution' (2012) 17 *J of Conflict and Security L* 229, especially at 234.

93 This doctrine, of course, concerns liability of a State for actions of its own official agents; the position is more complicated where the wrongful acts are committed by non-State actors. See generally Malcom N Shaw, *International Law* (CUP 2008) 785–93.

94 *Corfu Channel (United Kingdom v Albania) (Merits)* (Judgment) [1949] ICJ Rep 4, 18.

command network of an opposing belligerent, before leaving neutral territory. All this could occur within a period of 24 hours or less. How precisely could the neutral State's authorities reasonably be expected to prevent or terminate such activity without leaving the door open to an aggrieved belligerent to take hostile action against the neutral State? The ICJ stated further in the *Corfu Channel Case* that in light of a victim State's frequent inability to furnish direct proof of facts disclosing responsibility for a breach of international law, '[s]uch a State should be allowed a more liberal recourse to inferences of fact and circumstantial evidence'.[95] The formula adopted by the International Group of Experts in the Tallinn Manual is consonant with that dictum and would seem to entail a presumption very much in favour of an 'aggrieved belligerent's' rights, to the detriment of those of a neutral.

The content of Rule 154 would be of interest in the event of the UN Security Council ordering action against a delinquent State that was engaging in cyber operations that were deemed a threat to the peace, breach of the peace or act of aggression, in terms of Chapter VII of the UN Charter. The suggestion is that in such a situation, it would not be a breach of a neutral State's obligations under the law of neutrality for it to participate in cyber operations ordered by the Council,[96] consistent with Article 42 of the Charter. Presumably, if the Council ordered 'cyber sanctions' consistent with Article 41, a neutral State could be called upon to comply with them in accordance with its duty to accept and carry out Council decisions under Article 25 – which, by virtue of Article 103, would override any inconsistent obligations arising under neutrality law. In practice, it remains to be seen how – if at all – neutral States would wish to 'stand on their neutrality', or otherwise, in such situations. The precedents set during the First Gulf War[97] suggest that there will be a divergence of opinion between those States that wish to insist on maintaining an attitude of neutrality (i.e., those most closely affected by the enforcement action) and those that are participating in any 'coalition of the willing' authorised by the Security Council. Taking the interconnectivity of the cyber domain into account, however, and the mutual interdependence that it implies, one may wonder whether it will not be the case that all 'heavily wired' States might not come to view themselves as being closely affected by any cyber sanctions or cyber enforcement action.

(d) Selected Issues: *Jus in Bello*

A far larger number of provisions of the law of armed conflict (LOAC) potentially implicate neutrality in the cyber context than is the case in respect of the rules on the legality of the use of force by States, and there is a correspondingly greater number of legal provisions in the Hague Conventions V and XIII, and other 'musty' instruments, that might provide useful analogies for the application of neutrality law in the cyber age. Of particular interest are the various provisions relating to the construction and use of communications equipment on neutral territory, and those – even less well-known – from the Hague Rules for the Control of Radio in Time of War,[98] covering radio stations and apparatus. Although imperfectly fitted to the technology of cyber, these provisions from the first three decades of the twentieth century, with their focus

---

[95] Ibid.

[96] Tallinn Manual 2.0 (n 39) rule 154 para 3.

[97] Above, text accompanying nn 71–74.

[98] The Hague Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare, Part I: Rules for the Control of Radio in Time of War (n 27) 33.

on what were then modern means of communication, represent perhaps the closest analogies in settled international law to the types of issues likely to be encountered by neutral States in the cyber domain.[99] On land, belligerents are forbidden to erect on neutral territory 'a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces',[100] or to use for purely military purposes any such apparatus erected before a conflict if it is not 'opened for the service of public messages'.[101] There is a duty on neutral States not to allow any of these acts to occur on their territory,[102] but they are not required to forbid or restrict belligerent use of any telegraph, telephone cables or wireless telegraphy apparatus situated on their territory, irrespective of whether such devices belong to the State itself, to companies or to private individuals.[103] The erection of 'wireless telegraphy stations or any apparatus for the purpose of communicating with the belligerent forces' is equally forbidden in neutral ports and territorial waters.[104] Special provisions regarding radio stations are enumerated in the Hague Rules for the Control of Radio in Time of War, although it must be remembered that this instrument was never formally adopted as a binding treaty or opened for signature or ratification. The erecting or operation, by belligerents or their agents, of radio stations 'within neutral jurisdiction' is stated to be a violation of neutrality; it is worth noting that this was not limited to conduct by belligerents but is equally a violation if a neutral State permits it to happen.[105] In keeping with similar provisions in Hague Convention V, neutral States were not required to restrict or prohibit the use of radio stations within their jurisdiction, except in order to prevent transmission of information.[106] In a provision of particular interest in the cyber context, the use of mobile radio stations belonging to belligerents was also addressed: these were not to be used while within neutral jurisdiction and neutral States were required to employ 'the means at their disposal' to prevent such use;[107] and mobile radio stations belonging to neutrals were not to keep any record of messages received from belligerent radio stations, 'unless such messages are addressed to [the neutral stations] themselves'.[108]

What are we, some 100 years later in the age of the Internet, to make of these almost extravagantly archaic provisions, and how – if, indeed, at all – are we to 'fit' them to the possibilities of cyber conflict?[109] There are in fact some fairly clear analogies that can usefully be drawn. Computers undoubtedly form part of cyber infrastructure and are therefore analogous to wireless telegraphy, for instance; facilities housing networked computers could be considered similar to radio stations; computer viruses, malware, botnets and other similar tools for cyber

---

[99] See, generally, Jeffrey T Kelsey, 'Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare' (2008) 106 *Michigan L Rev* 1427, 1441–6.

[100] HC V, art 3(a).

[101] Ibid., art 3(b).

[102] Ibid., art 5.

[103] Ibid., art 8.

[104] HC XIII, art 5.

[105] The Hague Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare, Part I: Rules for the Control of Radio in Time of War (n 27) art 3.

[106] Ibid., art 4.

[107] Ibid., art 5.

[108] Ibid., art 8.

[109] For an elaborate but far from unrealistic example of a possible scenario involving neutrality in cyber conflict, see Eric T Jensen, 'Sovereignty and neutrality in cyber conflict' (2012) 35 *Fordham Intl L J* 815, 816–17.

war could be likened to means of warfare within the meaning of LOAC.[110] Technicians who operate computer systems on behalf of belligerents while on neutral territory could be lawful combatants or civilians directly participating in hostilities, depending on their personal status under LOAC.[111]

The main emphasis in the Hague Conventions and Rules is on the protection of neutral territorial sovereignty and jurisdiction on the one hand, and the prohibition of communications with belligerents on the other. As to the former, it is probable that jurisdiction will be more significant in the cyber age than territory per se: cyberspace is not part of any tangible territory – unlike airspace, it cannot even be classified according to its proximity to land or water[112] – so it is difficult to see how the territorial location of cyber violations can be ascertained (particularly in light of the difficulties of attribution and as regards the use of mobile infrastructure like laptop computers) other than by reference to the concept of jurisdiction.[113] It was stated more than 30 years ago in connection with an American attempt to exercise jurisdiction in respect of the export, by third States, of US-derived technical data to the Soviet Union: 'Goods and technology do not have any nationality and there are no known rules under international law for using goods or technology situated abroad as a basis of establishing jurisdiction over the persons controlling them.'[114] On the other hand, 20 years later, things had moved on enough for criminal jurisdiction to be included in a new treaty relating to certain aspects of cyber activity.[115] We must also bear in mind the very fluid, intangible nature of the Internet, and the fact that the types of acts which could constitute violations of cyber neutrality are likely to be transnational in nature: hostile data could be transmitted from a network in one State and transit the Internet nodes or hubs of one or more intervening States before arriving at its target. It seems probable that in the future, States may seek to assert their cyber jurisdiction by reference, not to a concept of *territoriality* as emphasised in the Hague Conventions and Rules, but to one of *personality* – that is to say, the identity of the person(s) committing a cyber violation of neutrality may come to be seen as more useful legally than the location where the act occurs.[116] This may be an especially attractive legal possibility when one considers the ban on forming 'corps of combatants' on neutral territory in order 'to assist the belligerents'.[117] Given

---

[110] Thus, they could be analogous to 'munitions of war', in which case their movement 'across the territory' of a neutral State would be forbidden: HC V, art 2.

[111] See Tallinn Manual 2.0 (n 39) rules 86–91.

[112] A better analogy for cyberspace in fact would be outer space, which under public international law is considered *res communis* – an area which by definition is not capable of forming part of the territory of any State: see Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, UN Doc A/RES/2222 (XXI) (19 December 1966) Annex, arts I and II. An appropriate analogy may also be drawn with the high seas: see George K Walker, 'Information warfare and neutrality' (2000) 33 *Vanderbilt J of Transnational L* 1079, 1150–6.

[113] As to which generally, see Christopher Staker, 'Jurisdiction' in Malcom D Evans (ed), *International Law* (OUP 2018) 289.

[114] European Communities: Comments on the U.S. Regulations Concerning Trade with the U.S.S.R. (1982) 21 *International Legal Materials* 891, 894.

[115] See Convention on Cybercrime (Council of Europe), CETS No. 185, 23 November 2001 (entered into force: 1 July 2004) art 22.

[116] For further technical and jurisdictional possibilities, and very interesting discussion, see Thomas Schultz, 'Carving up the Internet: Jurisdiction, legal orders and the private/public international law interface' (2008) 19 *EJIL* 799. See also Tsagourias (Ch 1 of this Handbook).

[117] HC V, art 4.

the plausible deniability of much State involvement with malicious activity in cyberspace, and the assertions that so-called 'patriotic "hacktivists"' in Russia were responsible, for example, for DDOS attacks and webpage defacement in Estonia (2007) and Georgia (2008),[118] there could conceivably be scope for a revival, in the cyber context, of the concept of the *levée en masse*[119] found in the law of armed conflict.[120] Whether 'hacktivists' are legally considered civilians directly participating in hostilities or part of a *levée en masse*, however, they could arguably fall within the spirit of the prohibition in Article 4 of HC V.

As to communications with belligerents, this is likely to be of relevance primarily in the context of cyber espionage;[121] an activity which is neither expressly permitted nor expressly prohibited under public international law; despite the probability that it would violate the international law of neutrality, it is more likely to be treated as a violation of national law only, particularly since under LOAC it is defined as occurring in the territory of a party to a conflict (as opposed to a neutral).[122] Finally, it may be noted that the use of infrastructure is not prohibited or necessarily restricted if it is *the neutral State's own infrastructure*:[123] so by analogy the use of computers, servers or Internet Service Providers belonging to a neutral State, on behalf of belligerents, would not be forbidden. It remains arguable, however, that the use in neutral territory of a laptop belonging to a belligerent State or one of its nationals in order to assist that belligerent in active hostilities would be considered a violation of neutrality law.

4. CONCLUSION

In the early stages of World War II the principal concerns of neutral nations were overwhelmingly to do with the protection of their territorial sovereignty against violation. They involved such matters as protesting against the shining of searchlights from British warships into territorial waters at night (in the case of Norway)[124] and ensuring the departure of the damaged German pocket battleship *Admiral Graf Spee* from the neutral harbour of Montevideo after the Battle of the River Plate, which itself had taken place within a neutral exclusion zone unrecognised by the belligerents (in the case of Uruguay).[125] In the early twenty-first century the main equivalent issues of preoccupation are likely to be routing or transit of cyber attacks

---

[118] See Piret Pernik, 'Different tactics, same story' (28 March 2014) *RKK/CDS blog*, http://blog.icds.ee/article/255/different-tactics-same-story.

[119] As most recently defined in Geneva Convention (III) Relative to the Treatment of Prisoners of War of August 12, 1949 (1950) 75 UNTS 135–285, art 4(A)(6). See also Arimatsu (Ch 19 of this Handbook) and Bannelier (Ch 20 of this Handbook).

[120] But see Tallinn Manual 2.0 (n 39) rule 88. The Commentary to a subsequent rule then makes it clear that the Experts regard 'hacktivists' as civilians directly participating in hostilities: ibid., rule 97 para 12. See also David Turns, 'Cyber warfare and the notion of direct participation in hostilities' (2012) 17 *J of Conflict and Security L* 279.

[121] See Buchan and Navarrete (Ch 11 of this Handbook).

[122] Tallinn Manual 2.0 (n 39) rule 89, para 7. Such activities conducted outside enemy controlled territory would in fact more correctly be classified as computer network exploitation or cyber reconnaissance, doctrinal concepts which in no way violate international law.

[123] HC V, art 8.

[124] See Simpson (n 4) 219.

[125] For a summary of the battle, its background and consequences: see Sydney D Waters, *The Royal New Zealand Navy* (Historical Publications Branch 1956) 45–74.

via Internet servers, nodes or other infrastructure located in or owned by neutral States; thus, the territorial link remains, despite the intangible nature of the domain. Particular questions are likely to involve the extent of awareness of the neutral State's authorities about any cyber infringement of their neutrality; whether those authorities have the ability to prevent such infringements from occurring; the source and routing of cyber attacks; and to whom such infringements are attributable. The same principles as were applicable 100 years ago – the Hague Conventions and customary international law – remain applicable today, by analogy if not directly. While the literature on cyber war and international law generally is now rather extensive and national legal doctrine increasingly includes coverage of cyber issues, the focus in terms of the application of the law to cyber activities in armed conflicts has been squarely on such operational topics as legitimate targets and precautions in attack, there has been almost nothing in the way of addressing specific aspects of neutrality law and its application in the context of cyber war. Rare exceptions are to be found in relation to the protection of submarine cables,[126] the law of blockade,[127] and the right of a neutral State to 'protect its neutrality by impeding the use of infrastructure and systems (e.g. botnets) by [belligerents] on [its] territory';[128] but there remains a complete dearth of State practice in actual contemporary cyber conflicts.

It would not be unreasonable to assume that the ever-greater interconnectedness of nations' affairs, economically and politically, and their increasing mutual interdependence, as well as the all-pervasive nature of the Internet and cyber networks and the increasing evidence of hostile cyber operations – albeit at a low level, short of armed conflict – may well lead those States that do not wish to become embroiled in such situations to emphasise and reinforce their adherence to neutrality law; this may well be so, even in situations where the international community, acting through the UN Security Council, has clearly designated an aggressor and ordered collective security enforcement action. It is therefore entirely possible, the lack of recent and current State practice notwithstanding, that the international law of neutrality may yet undergo its biggest renaissance since those days of neutral waters and searchlights in a less wired world. As has been suggested, 'Undeniably, neutrality as a general concept has as much vitality today as in the pre-Charter era… [the] opportunity for claims of neutrality… remains large.'[129]

---

[126] James Kraska, 'The Law of Maritime Neutrality and Submarine Cables' (29 July 2020) EJIL: *Talk!*, https://www.ejiltalk.org/the-law-of-maritime-neutrality-and-submarine-cables/.

[127] New Zealand Defence Force, *Manual of Armed Forces Law, Law of Armed Conflict*, DM 69 (2 ed) Volume 4, § 8.10.25.

[128] See Marten Zwanenburg and Nelleke van Amstel, 'The Netherlands' (*YIHL Correspondents' Reports* Vol. 15, 2012, 2) https://www.asser.nl/asserpress/documentation/yihl-correspondents-reports-2012/.

[129] Walker (n 112) 1197.

23. European law and cyberspace

Ramses A. Wessel

1. INTRODUCTION: DEFINING EU CYBERSECURITY LAW

Does anything like cybersecurity law exist as part of European Union law? Cybersecurity is not mentioned as such in the EU Treaties as an area to be dealt with by the EU. This should not come as a surprise. After all, while security reasons where behind the creation of the original European Communities in the 1950s, the main means were economic in nature. Nevertheless, after a number of earlier policy initiatives,[1] cybersecurity is now high on the EU's agenda in particular since the adoption of the 2013 Cybersecurity Strategy (updated in 2017[2]) and the 2015 Council conclusions on cyber-diplomacy.[3] The Union's first legal act in the field of cybersecurity was adopted in 2016 in the form of a Directive on a common level of security of network and information systems.[4] More recently, in 2019, the EU adopted the EU Cybersecurity Act,[5] which aims to streamline various policies and relabelled the European Union Agency for Network and Information Security (ENISA) to the European Agency for Cybersecurity, while holding on to the original abbreviation.[6] The fact that the EU justified and clarified its legal activities in this area in a 110-points preamble to the EU Cybersecurity Act points to an awareness that this is not obvious area to deal with from a legal perspective. At the same time, the proliferation of policy documents continues. On 24 July 2020, the European Commission published the latest addition to the collection of EU strategies, the new

[1] See for the early emergence of an EU policy on cybercrime from a comparative perspective: Fernando Mendez, 'The European Union and Cybercrime: Insights from Comparative Federalism' (2005) 12 *Journal of European Public Policy* 509; as well as Ramses A Wessel, 'Cybersecurity in the European Union: Resilience through Regulation' in Elena Conde Pérez, Zhaklin V Yaneva and Marzia Scopelliti (eds), *Routledge Handbook of EU Security Law and Policy* (Routledge 2019) 283–300. The present contribution further builds on that latter publication as well as on the chapter 'Towards EU Cybersecurity Law: Regulating a New Policy Field' in the 2015 edition of this Research Handbook and can be seen as an update of these earlier publications.

[2] European Commission, 'State of the Union 2017 – Cyber-security: Commission scales up EU's response to cyber-attacks', Press Release (Brussels, 19 September 2017).

[3] Respectively European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final (Brussels, 7 February 2013) http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf; and *A Digital Single Market Strategy for Europe*, COM(2015) 192 final (Brussels, 6 May 2015) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192.

[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

[5] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ EU L 151/15, 7.6.2019.

[6] https://www.enisa.europa.eu.

EU Security Union Strategy (SUS),[7] with, again, a strong emphasis on critical infrastructure protection and resilience and plans for a new a Joint Cyber Unit to provide structured and coordinated operational cooperation.

Despite the absence of a clear and concrete legal basis for the EU to act in this area, and despite the Union's traditional focus on other policy areas, the range of initiatives shows that 'cybersecurity is now among one of the EU's most important priorities, with cyber security elements having been integrated transversally within other EU policies'.[8] The reasons are obvious: over the past years the number of cyber-attacks on States and critical infrastructure have been constantly growing,[9] and by its nature cybersecurity needs cross-border cooperation.[10] The EU measures aim to build resilience, fight cybercrime, build cyberdefence, develop industrial and technical resources and elaborate a diplomatic strategy for cyberspace.[11] Indeed, 'resilience' is a key-word in the EU's 2016 Global Strategy,[12] and this strategy seems more clearly aimed at responding to threats than at promoting values, as was the case in the 2013 Security Strategy. Cybersecurity is now presented as a key-element in the EU's security and resilience policies,[13] albeit that the Union's role is largely limited to 'coordinate', 'support', or 'assist' its Member States in this area due to the lack of express competences. That the Union is aware of this, is underlined in the 2019 Cybersecurity Act: 'This Regulation is without prejudice to the competences of the Member States regarding activities concerning public

---

[7] EU Security Union Strategy, COM(2020) 605 final, Brussels, 24.7.2020; https://ec.europa.eu/info/sites/info/files/communication-eu-security-union-strategy.pdf.

[8] Helena Carrapico and André Barrinha, 'European Union Cyber Security as an Emerging Research and Policy Field' (2018) 19 *European Politics and Society* 299, 300. See for a recent overview of the initiatives also Gloria González Fuster and Lina Jasmontaite, 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights' in Markus Christen *et al*. (eds), *The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology* (Springer 2020) 109; Faye F Wang, 'Legislative Developments in Cybersecurity in the EU' (2020) 1 *Amicus Curiae* 233; Agnes Kasper and Alexander Antonov, 'Towards Conceptualizing EU Cybersecurity Law' (2019) *ZEI Discussion Paper* C253; as well as George Christou, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (Palgrave MacMillan 2016).

[9] See https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018; as well as Kasper and Antonov (n 8); Annegret Bendiek, *European Cyber Security Policy* (2012) *SWP Research Paper* 13; as well as Jed Odermatt, 'The European Union as a Cybersecurity Actor' in Steven Blockmans and Panos Koutrakos (eds), *Research Handbook on EU Common Foreign and Security Policy* (Edward Elgar 2018). Also, see the earlier report by Neil Robinson *et al*., *Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts* (European Parliament, Directorate-General for Internal Policies, Policy Department A: Economic and Scientific Policy, September 2013).

[10] *Cf* already the remarks by the European Commission in 2011 that cybercrime is 'by its very nature cross-border' and hence 'proper cross-border arrangements' are required. Commission Communication on Critical Information Infrastructure - results and next steps: the path to global security network, 3.12.2011, COM (2011) 163 final.

[11] Annegret Bendiek, 'A Paradigm Shift in the EU's Common Foreign and Security Policy: From Trans-formation to Resilience' (October 2017) *SWP Research Paper*.

[12] See *Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy*, 2016; https://europa.eu/globalstrategy/en.

[13] The term 'cyber' appears 23 times in the EU's Global Strategy. See more in general also George Christou, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (Palgrave MacMillan 2016).

security, defence, national security and the activities of the State in areas of criminal law'.[14] Clearly showing the tension between the existence of national competences and the need for the EU to act, it adds the following:

> Cyberattacks are on the increase and a connected economy and society that is more vulnerable to cyber threats and attacks requires stronger defences. However, while cyberattacks often take place across borders, the competence of, and policy responses by, cybersecurity and law enforcement authorities are predominantly national. Large-scale incidents could disrupt the provision of essential services across the Union. This necessitates effective and coordinated responses and crisis management at Union level, building on dedicated policies and wider instruments for European solidarity and mutual assistance.[15]

These words underline the need for the EU to adapt its security strategy to new threats.[16] Perhaps ironically this has to be done in a period in which traditional EU defence cooperation finally seems to be progressing. After decades of attempts to establish a defence cooperation alongside the EU's other policies, the careful introduction of the Common Security and Defence Policy (CSDP) in the 1992 Maastricht Treaty and its further adaptations through subsequent treaty revisions,[17] we now witness new and far-reaching initiatives, including the implementation of the notion of permanent structured cooperation (PESCO), new structures and frameworks, enhanced oversight and coordination mechanisms as well as financing tools to trigger joint defence research and development.[18]

The fact that the EU does not have an express competence to take measures to improve cybersecurity has led it to either use legal competences it has in other areas, or adopt soft-law and coordination measures (see section 3). This piecemeal approach has made it difficult to understand what exactly is covered by cybersecurity and, on that basis, to allocate tasks and responsibilities.[19] As underlined by Fuster and Jasmontaite: 'Definitions used to refer to cybersecurity by various actors, including EU Member States, bodies and institutions, typically represent different perspectives, which can potentially be at odds with each other'.[20] And, central to the present chapter is the idea that '[t]he lack of clarity about this core concept raises

---

[14] EU Cybersecurity Act 2019, Art 1(2).

[15] Ibid., preamble, point 5.

[16] Bendiek (n 9) 5.

[17] See for a recent overview Ramses A Wessel and Joris Larik (eds), *EU External Relations Law: Text, Cases and Materials* (Hart 2020) Chapter 12.

[18] See further on these initiatives the PESCO Factsheet: https://eeas.europa.eu/headquarters/headquarters-Homepage/34226/permanent-structured-cooperation-pesco-factsheet_en; as well as Steven Blockmans, 'The EU's modular approach to defence integration: An inclusive, ambitious and legally binding PESCO?' (2018) 55 *Common Market Law Review* 6, 1785–826.

[19] *Cf* Odermatt (n 9); as well as Krystof F Sliwinski, 'Moving Beyond the European Union's Weakness as a Cyber-Security Agent' (2014) 35 *Contemporary Security Policy* 468, 470:

> There is no coherent European understanding of what the notion of cyber-security should include. Consequently, conceptualization differences are more than likely to produce different approaches to respective national capabilities catalogues. Such inconsistencies, when reinforced by national security narratives and traditional sovereignty claims, are more than likely to leave the EU toothless in the future…

See also Federica Di Camillo and Valérie Miranda, 'Ambiguous Definitions in the Cyber Domain: Costs, Risks and the Way Forward', Working Paper No. 11, IAI 26 September 2011.

[20] Fuster and Jasmontaite (n 8) 104.

questions about coherence and consistency of already adopted and newly proposed legislative acts in the field of cybersecurity'.[21]

The definition of cybersecurity that was included in the 2013 Cybersecurity Strategy of the European Union (EUCSS) has a broad scope:[22]

> *Cyber-security* commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.

A narrower definition was provided in the context of the 2019 Cybersecurity Act: '"cybersecurity"means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats'. This relates to ensuring the resilience of networks to potential attacks and the capacity to respond to such attacks.

Yet, cyberspace policies usually also include 'cybercrime'. Indeed, both the broader notion of 'cybersecurity' and the criminal activities falling under 'cybercrime' form part of the EU's policies.[23] In the 2013 EU Strategy it is described as follows:

> *Cybercrime* commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware).

Hence, while *cybersecurity* refers to the range of safeguards and actions that can be used to protect the cyber domain, *cybercrime* reflects to the actual criminal activities, thus following the descriptions laid down in the Council of Europe Convention on cybercrime.[24] Debates on activities in cyberspace also refer to many more phenomena. Where cybercrime involves offences against property rights of non-State actors (e.g., phishing), *cyber espionage* concerns breaches in the databases of State or non-State enterprises by foreign government agencies, and *cyber war* involves State attempts to attack another State via electronic networks.[25] Given the Union's activities under the heading of its CSDP, it is striking that the latter is hardly

---

[21] Kasper and Antonov (n 8).

[22] Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', 7 February 2013 ('EUCSS').

[23] See for a discussion on definitional questions also Elaine Fahey, 'The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security' (2014) 5 *European Journal of Risk Regulation* 46: 'Conceptually, cybercrime may be defined both narrowly, to include offences against computer data and systems but also more broadly, to include offences committed with the help of computer data and systems. By contrast, cyber-security usually relates to four major societal threats – crime, cyberwar, cyber terrorism and espionage…' (at 47).

[24] Convention on Cybercrime, CETS No. 185, Council of Europe, signed 23 November 2001 in Budapest, entry into force 1 July 2004.

[25] On cyber espionage see Buchan and Navarrete (Ch 11 of this Handbook) and on cybercrime see Kastner and Mégret (Ch 12 of this Handbook). *Cf* Annegret Bendiek and Andrew L Porter, 'European Cyber Security Policy within a Global Multistakeholder Structure' (2013) 18 *European Foreign Affairs*

mentioned in the EU's documents on cybersecurity. Indeed, allegedly for reasons of Member State sovereignty in the military field, the term *cyberdefence* lacks a clear definition in the EU context.[26]

The aim of the present chapter is to provide an introduction into the ways in which the EU aims to play a role in the regulation of cybersecurity, both in relation to its own Member States as in contributions to global law-making and governance. Section 2 starts with presenting the internal objectives of the Union as well as its global ambitions in this area. This is followed by an analysis of existing legal competences in Section 3. Section 4 will draw some conclusions.

2. EU GLOBAL AND INTERNAL OBJECTIVES OF CYBERSECURITY

As noted above, with the adoption of the 2016 *Global Strategy for the European Union's Foreign and Security Policy* the EU stressed the importance of 'resilience'.[27] In fact, the term is used more than 30 times in the 60-page Global Strategy, turning 'resilience' into a key objective of the EU security strategy. While the term as such is not defined by the Global Strategy, the context makes clear that the main ambition is to resist and overcome threats to the EU's security and democratic values:[28] 'The Strategy nurtures the ambition of strategic autonomy for the European Union. This is necessary to promote the common interests of our citizens, as well as our principles and values.'[29] Yet, the idea of autonomy should not be read as to isolate the EU. On the contrary: 'Together with its partners, the EU will [also] promote resilience in its surrounding regions.'[30] And, this is done in cooperation with international partners. Thus, the EU Cyber Defence Policy Framework, for instance, clearly refers to cooperation with other international organizations, including NATO.[31] In addition, cybersecurity and cyber-defence cooperation between the EU and NATO has been intensified since 2015, formalised in the July 2016 Warsaw Declaration, and reinforced with concrete implementation proposals at the joint meeting of the EU and NATO foreign ministers in December 2016.[32] More generally, the

---

Review 155, 158. This article also provides a good overview of the wide scope of the actual problems caused by a lack of cybersecurity.

[26] George Christou, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (Palgrave MacMillan 2016) 6: 'Cyber defence is not defined within the EU documents given the sensitivity among member states on this issue, and the reluctance of certain member states to participate given their own cyber defence strategies.'

[27] See also Bendiek (n 11) 6.

[28] As phrased by the Global Strategy (n 12) 21, it is about 'the swift recovery of Members States in the event of attacks'. See also Bendiek (n 11) 6:

> Resilience is generally understood as 'a capacity to resist and regenerate', as well as be 'crisis-proof'. The concept acknowledges that there are practical limits to the normative goal of external transformation as outlined in article 21 paragraph 2 of the TEU. Resilience therefore aims to enable the EU both to maintain its existing values and norms and to pursue its own interests.

[29] EU Global Strategy (n 12) 4.

[30] Ibid., 23.

[31] Cyber Defence Policy Framework, Brussels, 19 November 2018 14413/18; https://www.consilium.europa.eu/media/37024/st14413-en18.pdf. See further also Bendiek (n 11) 18.

[32] Ibid; and Bruno Lété and Daiga Dege, *NATO Cybersecurity: A Roadmap to Resilience*, Policy Brief 3, 2017 (Washington: The German Marshall Fund of the United States, July 2017).

Union has engaged in a number of strategic partnerships with third countries, also as part of its strategy to 'mainstream' cyber issues in the EU's external relations.[33]

In joining the large group of global governmental and non-governmental actors active in the governance and regulation of cybersecurity,[34] the EU commits again to its traditional role as a normative actor, in line with its brief in Articles 3(5) and 21 of the Treaty on European Union.[35] While the EU is sometimes successful in getting its standards accepted by many other countries – as exemplified by the European General Data Protection Regulation (GDPR)[36] – developing its own rules and standards may also contribute to the current fragmentation in actors, definitions and norms characterizing the current global regime in this field.[37]

In any case, any possible contribution to the global regulation of cybersecurity very much depends on the internal activities the EU is engaged in. In order to understand the EU's ambitions and plans related to cybersecurity, it is useful to quote the respective paragraph in the Global Strategy in full:

> The EU will increase its focus on cyber security, equipping the EU and assisting Member States in protecting themselves against cyber threats while maintaining an open, free and safe cyberspace. This entails strengthening the technological capabilities aimed at mitigating threats and the resilience of critical infrastructure, networks and services, and reducing cybercrime. It means fostering innovative information and communication technology (ICT) systems which guarantee the availability and integrity of data, while ensuring security within the European digital space through appropriate pol-

---

[33] Thomas Renard, 'EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain' (2018) 19 *European Politics and Society* 321. Renard lists the following dialogues in the framework of strategic partnerships: Brazil (Dialogue on international cyber policy; Information society dialogue); Canada (EU-US-Canada Expert Meeting on Critical Infrastructure Protection China Cyber taskforce; Dialogue on IT, telecommunications and informatisation); India (Political dialogue on cyber-security; Information society dialogue); Japan (Cyber dialogue; Dialogue on ICT policy); Mexico (Working Group on telecommunications; Dialogue on public security and law enforcement); Russia (Information society dialogue South Africa Information society dialogue); South Korea (Cyber dialogue; Information society dialogue); USA (Working Group on Cyber-security and Cyber-crime (WGCC); Cyber dialogue; Information society dialogue; EU-US-Canada Expert Meeting on Critical Infrastructure Protection).

[34] In a recent study we came to a list of international institutions that at least includes the EU, the Council of Europe, the United Nations, the International Telecommunications Union (ITU), the African Union, Microsoft, the Internet Engineering Task Force (IETF), the International Organization for Standardization (ISO), NATO, Net Mundial, the G7, the Internet Governance Forum, the Electrical and Electronic Engineers (IEEE), the International Electro-technical Commission (IEC), ICANN, the Asia-Pacific Economic Cooperation (APEC), the Organization for Security and Co-operation in Europe (OSCE), the OECD, the G8, Interpol, the organization of American States (OAS), the Arab League and Gulf Cooperation Council, the International Multilateral Partnership Against Cyber Threats, the G20, the Shanghai Cooperation Organisation, the World Trade Organization (WTO), the World Intellectual Property Organization (WIPO), and UNESCO. See Tatiana Nascimento Heim and Ramses A Wessel, 'The Global Regulation of Cybersecurity: A Fragmentation of Actors, Definitions and Norms' in Lucía Millán Moro (dir.) and Gloria Fernández Arribas (ed), *Ciberataques y Ciberseguridad en la Escena Internacional* (Aranzadi Thomas Reuters 2020) 146–73.

[35] Rames A Wessel and Joris Larik, 'The EU as a Global Actor' in Ramses A Wessel and Joris Larik (eds), *EU External Relations Law: Text, Cases and Materials* (Hart 2020) 1–28.

[36] Giovanni Buttarelli., 'The EU GDPR as a clarion call for a new global digital gold standard' (2016) 6 International Data Privacy 77. See more generally, Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP 2020).

[37] See Nascimento Heim and Wessel (n 34).

> icies on the location of data storage and the certification of digital products and services. *It requires weaving cyber issues across all policy areas, reinforcing the cyber elements in CSDP missions and operations*, and further developing platforms for cooperation.[38]

Cybersecurity is thus presented as a 'cross-sectional' policy task, and should be a dimension of different EU policy areas related to both internal and external security and civilian as well as military cooperation.[39]

More concrete ambitions can be found in the *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*,[40] that addresses different dimensions of cybersecurity, including network and information security (NIS), cybercrime, and cyberdefence. The general starting point is the following: '*For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online*.'[41] The Cybersecurity Strategy can be seen as a continuation of the internal and external policies that have been developed by the EU in the area of NIS[42] – and in the framework of the EU-US Working Group on Cyber-Security and Cyber-Crime (WGCC).[43] The European Commission announced plans to update the Cybersecurity Strategy in 2020.[44] Part of the Cybersecurity Strategy is related to linking core EU values that exist in the 'physical world' to the 'digital world': promoting fundamental rights, freedom of expression, personal data and privacy; access for all; democratic and efficient multi-stakeholder governance and a shared responsibility to ensure security. Other elements relate to other policy areas of the EU, including the internal market or defence policy. As an express legal basis cannot be found in the EU Treaties, the Strategy acknowledges that 'it is predominantly the task of the Member States to deal with security challenges in cyberspace'.[45] It lists five strategic priorities: achieving cyber resilience; drastically reducing cybercrime; developing cyberdefence policy and capabilities related to the Common Security and Defence Policy; develop the industrial and technological resources for cybersecurity; and establish a coherent international cyberspace policy for the EU and promote core EU values.

Relying on a total of 27 Member States to take the necessary measures, however, again risks fragmentation. Primarily to overcome this risk, the European Agenda on Security (EAS) was adopted, as 'an effective and coordinated response at European level',[46] providing a strategic framework for EU initiatives in the field of cybersecurity. Specific policies in relation to

---

[38] Global Strategy, at 21–2; emphasis added.

[39] *Cf* also Bendiek (n 11) 18.

[40] See above.

[41] EU Cybersecurity Strategy (n 3) 1.

[42] *Inter alia* resulting in the 2001 Commission Communication on 'Network and Information Security: Proposal for a European Policy Approach' (COM(2001)298) and the 2006 'Strategy for a Secure Information Society' (COM(2006)251).

[43] EU-U.S. Summit 20 November 2010, Lisbon – Joint Statement, European Commission – MEMO/10/597 20/11/2010. See also Maria Grazie Porcedda, 'Transatlantic Approaches to Cyber-security and Cybercrime' in Patryk Pawlak (ed), *The EU-US Security and Justice Agenda in Action*, EUISS Chaillot Paper, No. 127, 30 December 2011; as well as Fahey (n 23).

[44] https://ec.europa.eu/digital-single-market/en/cyber-security.

[45] *Cf* also Emmanuel Darmois and Geneviève Schméder, 'Cybersecurity: a case for a European approach', SiT Paper SiT/WP/11/16; http://www.securityintransition.org/wp-content/uploads/2016/02/WP11_Cybersecurity_FinalEditedVersion.pdf.

[46] Communication from the Commission to the European Parliament, the Council, European Economic and Social Committee and the Committee of the Regions, European Agenda on Security, COM (2015) 185 final.

CSDP had already been formulated in the EU Cyber Defence Policy Framework,[47] to further integrate cybersecurity and defence into CSDP. The focus on these policies is on enhancing cyber-resilience of CSDP missions and operations through for instance standardized procedures and technical capabilities in both civilian and military missions and operations.

More recently, the Commission laid down the EU ambitions in a comprehensive 'cybersecurity package': *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*.[48] This policy document – sometimes referred to as the 2017 Joint Communication or the Second Cybersecurity Strategy – further analyses the way forward and introduces a large number of new policy initiatives and actions by the EU, but also calls upon Member States to, *inter alia*, ensure full and effective implementation of the NIS Directive; apply the same rules to public administrations, given the role they play in society and the economy as a whole; provide cybersecurity-related training in public administration; prioritise cyber-awareness in information campaigns and including cybersecurity as part of academic and vocational training curricula; and use initiatives on the 'Permanent Structured Cooperation' (PESCO) and the European Defence Fund to support the development of cyber defence projects.

Overall, the conclusion is that the EU is very active in developing policies related to all dimensions of cybersecurity, mainly by drafting policy frameworks and guidelines to enhance and synchronise Member State initiatives. The topic is clearly high on the agenda and the EU's ambition is to play a central coordinating role in this area. Indeed, with one main goal in mind: resilience through policy-making and regulation. These policies are more internal than external.[49] This implies, as also rightfully concluded by Odermatt, that 'Unlike some other states, the EU has not sought to develop any kind of hard or offensive cyber power. The EU's approach to cyberdefence is guided by the logic of protection'.[50] The fact that external competences often depend on the existence (and/or use) of internal competences,[51] has indeed limited the Union's legal powers as a global actor in this field.[52] This is not to say that the Union is completely passive in its external relations with regard to cybersecurity initiatives. It does see itself as 'a global digital player', that aims at mainstreaming 'digital issues' in its foreign policy (see also section 3 below).[53] The question remains, however, to what extent the EU has the legal competence to realize its internal as well as external ambitions.

3. EU COMPETENCES RELATED TO CYBERSECURITY

The EU is well placed to address cybersecurity, given the scope of its policies and the tools, structures and capabilities at its disposal. While Member States remain responsible for national security, the scale and cross-border nature of the threat make a powerful case for EU action providing incentives

---

47 www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

48 Joint Communication to the European Parliament and the Council, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, Brussels, 13.9.2017, JOIN(2017) 450 final.

49 The Cybersecurity Strategy even clearly states that 'The EU does not call for the creation of new international legal instruments for cyber issues' (at 15).

50 Odermatt (n 9).

51 *Cf* Wessel and Larik (n 17) Chapter 3.

52 See Renard (n 33) 326: 'But just like in many other policy areas, the EU aims to assert itself in the global arena through 'soft power' assets and diplomatic skills'.

53 See Europe as a Global Digital Player; https://ec.europa.eu/digital-single-market/en/content/europe-global-digital-player.

> and support for Member States to develop and maintain more and better national cybersecurity capabilities, while at the same time building EU-level capacity.[54]

Irrespective of this statement by the European Commission, the question is whether also in a legal sense, the EU is 'well placed' to address cybersecurity.[55] Given the inherent cross-border nature of cybersecurity, the complete absence of the issue in the EU treaties is striking and was not even part of the 2009 treaty update. One reason may be that cooperation by the EU Member States or a transfer of competences to the EU may not be sufficient, precisely because of the larger, global scope of the challenge and the involvement of multiple actors.[56] Yet, given the EU's ambitions described in the previous section, concrete legal bases to at least also formally regulate cybersecurity need to be found. After all, the EU, like other international organizations, fully depends on an attribution of competences, not only for its internal activities, but also for engaging in cooperation with other States and international institutions.[57] And in the absence of express powers, these will need to be found in relation to other policy sectors. This was also emphasized by the European Parliament:

> conflicts and crises in Europe and around are happening in both physical and cyber space, and underlines that cyber security and cyber defence must therefore be integrated as the core elements of the CSDP and fully mainstreamed throughout all the EU's internal and external policies.[58]

Whereas this is understandable, it also entails a risk of fragmentation and inconsistency when different EU (and Member States') institutions, as well as private actors (industry, service

---

[54] 2017 Joint Communication to the European Parliament and the Council.

[55] The Union's activities partly build on the EU's engagement with the regulation of the Internet in a broader sense – with co-regulation as an important dimension. See for instance Franz C Mayer, 'Europe and the Internet: The Old World and the New Medium' (2000) 11 *European Journal of International Law* 149. See also Christopher T Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (CUP 2011).

[56] *Cf* Jan Kleijssen and Pierluigi Perri, 'Cybercrime, Evidence and Territoriality: Issues and Options' (2016) 47 *Netherlands Yearbook of International Law* 147. Indeed, as mentioned by the authors, the Council of Europe in particular has been used to draft (even more broadly accepted) instruments, such as the 2001 Budapest Convention on Cybercrime (ETS No. 185) as well as a large number of treaties on international co-operation in criminal matters, including in particular the European Convention on Mutual Assistance in Criminal Matters (ETS No. 030), its Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 099), and the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 182). *Cf* also Bendiek and Porter (n 25).

[57] *Cf* also Art 5(2) TEU: 'Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States'. Indeed, the 'principle of conferral' may further complicate things and leaves the Union with two options: it either connects cybersecurity to existing competences in other fields, or it uses soft law instruments to stimulate Member States and other relevant actors to implement parts of its strategies. See on the various competence problems in relation to the cooperation of the EU with other international organizations: Ramses A Wessel and Jed Odermatt, *Research Handbook on the European Union and International Organizations* (Edward Elgar 2019).

[58] See also: European Parliament, European Parliament Resolution of 23 November 2016 on the Implementation of the Common Security and Defence Policy, 2016/2067(INI) (Strasbourg, 23 November 2016) http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2016-0440&language=EN.

providers, etc.) are involved, all with their own policy preferences and procedures. It is questionable whether the demands for consistency and effectiveness (Arts 13 and 21 TEU) can be met. Cybersecurity forms an excellent example of an area in which the different policy fields of the Union need to be combined (a requirement for *horizontal* consistency), and where measures need to be taken at the level of both the EU and the Member States (calling for *vertical* consistency). This possible fragmentation thus raises the question to what extent the above-mentioned ambitions aimed at ensuring 'resilience through regulation' can actually be attained, both internally and in the framework of the EU's external relations.

In an institutional sense, a number of initiatives have been taken to create specialized bodies, but again in specific fields only.[59] Thus, a special EU Cybercrime Centre (EC3) was established[60] and located at one of the EU's agencies, Europol in The Hague.[61] EC3 officially commenced its activities on 1 January 2013 with a mandate to tackle the following areas of cybercrime:

a. That committed by organized groups to generate large criminal profits such as online fraud
b. That which causes serious harm to the victim such as online child sexual exploitation
c. That which affects critical infrastructure and information systems in the European Union.

EC3 thus aims to become the focal point in the EU's fight against cybercrime, through building operational and analytical capacity for investigations and cooperation with international partners in the pursuit of an EU free from cybercrime. It publishes the yearly Internet Organised Crime Threat Assessment (IOCTA) on key findings and emerging threats and developments in cybercrime.[62] Yet, for the development of actual legislation, it is necessary for the European Commission and the European External Action Service (EEAS) to be involved. For that reason EC3 liaison offices have been placed at those institutions and to other relevant agencies, including ENISA, the EU Cybersecurity Agency.[63] This latter agency is located in Greece and has now become the main body in this field and it also works to improve cooperation between Member States to implement emergency response plans, conduct regular emergency drills, and develop systems to guard against attacks on critical infrastructure.[64]

Overall, however, it is questionable whether this somewhat loose institutional framework will allow the Union to regulate the field of cybersecurity in any comprehensive fashion. The following sub-sections will provide some examples of legal bases used to tackle different dimensions of cybersecurity.

---

[59] See on the institutional developments also Jukka Ruohonen, Sami Hyrynsalmi and Ville Leppänen, 'An Outlook on the Institutional Evolution of the European Union Cyber Security Apparatus' (2016) 33 *Government Information Quarterly* 746.

[60] Council conclusions on the establishment of a European Cybercrime Centre, 3172nd Justice and Home Affairs Council meeting Luxembourg, 7 and 8 June 2012.

[61] See https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

[62] See https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2.

[63] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance), OJ L 77, 13.3.2004.

[64] https://www.enisa.europa.eu/.

(a) The Single Digital Market

In terms of EU competences, a number of measures with an economic dimension fall under initiatives in the framework of the so-called 'Single Digital Market' (DSM). The Digital Single Market strategy was adopted on the 6 May 2015. It includes 16 specific initiatives which have been delivered by the Commission by January 2017.[65] The EU refers to an obvious economic element, which relates to the completion of the DSM: citizens need trust and confidence to engage in new connected technologies and to use e-commerce facilities.[66]

Indeed, the extensive internal market competences of the Union do provide some hooks for cybersecurity measures related to the functioning of the free movement or competition rules. This, for instance allows the Union to harmonize national rules with a view to the functioning of the internal market. A concrete example is formed by using the 'internal market harmonisation' provisions in Article 114 TFEU, as was done to find a legal basis for the Directive on Security of Network and Information Systems ('NIS Directive').[67] The NIS Directive forms the first piece of EU-wide legislation on cybersecurity, aimed at boosting the overall level of cybersecurity in the EU. Member States had to transpose the Directive into their national laws by 9 May 2018.[68] The Commission argued that under Article 114 TFEU, the EU can adopt 'measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market',[69] and security of network and information systems is seen as essential for the functioning of the internal market. The Directive presents the 'internal market' rationale as follows:

> Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market. […] Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security

---

[65] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A Digital Single Market Strategy for Europe*, Brussels, 6.5.2015, COM(2015) 192 final.

[66] See already much earlier the Electronic Commerce Directive, adopted in 2000, which introduced an Internal Market framework for electronic commerce, providing legal certainty for business and consumers alike. It established harmonized rules on issues such as the transparency and information requirements for online service providers, commercial communications, electronic contracts and limitations of liability of intermediary service providers. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000.

[67] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, 1 ('NIS Directive'). See also Johan David Michels and Ian Walden, 'Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?' (2020), *European Law Review*,; Dimitra Markopoulou, Vagelis Papakonstantinou, Paul de Hert, 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's role and the General Data Protection Regulation' (2019) *Computer Law & Security Review* 105336.

[68] See https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive.

[69] 'NIS Directive' (n 67) Explanatory memorandum.

> of network and information systems is therefore essential for the smooth functioning of the internal market.[70]

The Directive thus aims at setting a high common level of network and information security across the EU in a number of ways: 1. By requiring Member States to be adequately prepared for cyber threats. This involves the establishment of national NIS Strategies and national Computer Security Incident Response Teams (CSIRTs); and 2. by promoting cooperation between the Member States, e.g., through requirements for security and notification. The NIS Directive thus aims at securing resilience in certain critical sectors, including energy, health, transport and banking.[71] The involvement of the private sector – including a system for certification and labelling to achieve a functioning single market in cybersecurity – returns in the 2016 Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry.[72] Enhancing trust in the internal market is also pursued by the Regulation on electronic identification and trust services for electronic transactions in the EU internal market.[73] This Regulation is also based on Article 114 TFEU, which concerns the adoption of rules to remove existing barriers to the functioning of the internal market.

In general, these initiatives only seem to form the start of a range of new measures. The 2017 Mid-Term Review of the Single Digital Market process[74] listed a large number of contributing threats and reveals the complications the EU is facing, also in terms of competences: 'Cyberattacks are on the increase and tackling them faces the problem that while cyber-attacks are often cross-border, law enforcement competences are strictly national. […] This requires effective EU level response and crisis management, building upon dedicated cyber policies and wider instruments for European solidarity and mutual assistance.'

(b) Cybercrime

Another policy area in which the EU has been relatively active when it comes to the regulation of cybersecurity is 'cybercrime'. The 2005 Framework Decision on attacks against information systems is probably one of the first legal instruments adopted by the Union in relation to cybersecurity.[75] The main objective of that Decision was to improve cooperation between judicial and other competent authorities, including the police and other specialized law enforcement

---

[70] Ibid. Preamble, points 1 and 3.

[71] *Cf* also Odermatt (n 9).

[72] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the European Committee of the Regions, Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (2016) COM (2016) 410 final.

[73] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC; OJ L 257, 28.8.2014, 73–114.

[74] Communications from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy, *A Connected Digital Single Market for All*, Brussels, 10.5.2017, COM(2017) 228 final.

[75] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

services of the Member States, through approximating rules on criminal law in the Member States in the area of attacks against information systems. With a view to the integration of the former Police and Judicial Cooperation in Criminal Matters (PJCC) in the Union's Area of Freedom, Security and Justice (AFSJ), in August 2013 this Decision was replaced by the Directive on attacks against information systems (the 'Cybercrime Directive').[76] The legal basis of this Directive is Article 83(1) TFEU, which underlines that it forms part of the judicial cooperation in criminal matters, currently laid down in that part of the Treaty. In fact, this is one of the areas where one may find a competence of the EU to legislate in the area of cybercrime (despite the fact that the term is not used as such). Article 83(1) TFEU provides:

> The European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis.
>
> These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime.

The Cybercrime Directive establishes minimum rules on the definition of criminal offences and sanctions with respect to attacks against information systems.[77] It also provides minimum rules on the definitions of crimes included in the Directive.

Other instruments adopted in this area include the 2011 Directive on Combatting the Sexual Exploitation of Children Online and Child Pornography, the 2002 ePrivacy directive, ensuring the confidentiality of client information,[78] and the 2001 Framework Decision on combating fraud and counterfeiting.[79] In addition, new proposals have been issued in 2018 and 2019, including a Regulation and a Directive to facilitate law enforcement and judicial authorities to obtain the electronic evidence they need to investigate and eventually prosecute criminals and terrorists,[80] as well as a new Directive on non-cash means of payment, which updates the legal framework, removing obstacles to operational cooperation and enhancing prevention and victims' assistance, to make law enforcement action against fraud and counterfeiting of non-cash means of payment more effective.[81]

---

[76] See above.

[77] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, 8. This Directive replaced the 2005 EU Framework Decision on Attacks against Information Systems.

[78] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 OJ L 337, 18.12.2009, 11.

[79] Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, OJ L 149, 2.6.2001, 1.

[80] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final - 2018/0108 (COD); Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings COM/2018/226 final - 2018/0107 (COD).

[81] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA PE/89/2018/REV/3.

In terms of international cooperation, it is important to note that the EU is not a party to the main international treaty in this area, the Council of Europe Convention on Cybercrime (Budapest Convention),[82] although it participates in the Cybercrime Convention Committee (T-CY).

(c) Cyberdiplomacy

The EU's Common Foreign and Security Policy (CFSP) also does not explicitly address cybersecurity, Yet, Article 24(1) TEU provides that 'the Union's competence in matters of common foreign and security policy shall cover all areas of foreign policy and *all questions relating to the Union's security*'.[83] The latter part of this sentence indeed seems to allow for measures to be taken using CFSP as a legal basis.[84] While for a long time cybersecurity issues were not part of the EU's foreign policy, the EU recently adopted a framework for a joint EU diplomatic response to malicious cyber activities (the so-called 'cyber diplomacy toolbox'), which sets out the measures under the broader CFSP.[85] The instrument makes a start with listing, primarily, non-military instruments that could contribute to 'the mitigation of cybersecurity threats, conflict prevention and greater stability in international relations'.[86] Part of this initiative is an explicit extension of the EU's sanctions regime to cyber-attacks. In 2019 the Council adopted a Decision and a connected Regulation concerning restrictive measures against cyber-attacks threatening the Union or its Member States.[87] Taking restrictive measures falls under the Union's competence as laid down in Articles 29 TEU and 215 TFEU. The Decision 'applies to cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Union or its Member States'.[88] It relates to cyber-attacks aimed at critical infrastructure; services necessary for the maintenance of essential social and/or economic activities; critical State functions; the storage or processing of classified information; or government emergency response teams. EU Member States will have to take the measures necessary to prevent the entry into, or transit through, their territories of '(a) natural persons who are responsible for cyber-attacks or attempted cyber-attacks; (b) natural persons who provide financial, technical or material support for or are otherwise involved in cyber-attacks or attempted cyber-attacks, including by planning, preparing, participating in, directing, assisting or encouraging such attacks, or facilitating them whether by

---

[82] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. *Cf* also Mike Keyser, 'The Council of Europe Convention on Cybercrime' (2002–2003) *Journal of Transnational Law & Policy* 287.

[83] Emphasis added.

[84] See for a recent basic analysis of CFSP, Ramses A. Wessel, 'Common, Foreign, Security and Defence Policy' in Wessel and Larik (n 17) 283–326.

[85] See Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox'), Brussels, 7 June 2017 (OR. en) 9916/17.

[86] See Annegret Bendiek, 'The EU as a Force for Peace in International Cyber Diplomacy' (April 2018) 19 *SWP Comment*.

[87] Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I, 17.5.2019; and Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I, 17.5.2019; updated in 2020 by Council Decision (CFSP) 2020/651 of 14 May 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 153, 15.5.2020.

[88] Art 1 of the Decision.

action or omission; (c) natural persons associated with the persons covered by points (a) and (b)',[89] and funds of these persons and entities have to be frozen.[90] The mentioned Regulation spells out the rules in more detail and underlines that the rules are binding in each of the EU Member States. The first sanctions on the basis of the new regime were adopted on 30 July 2020, when four Russians were listed said to be guilty of trying to hack an international institute, the Organisation for the Prohibition of Chemical Weapons, in The Hague, in 2018. In addition, two Chinese men and a Chinese company were listed, in relation to the stealing of commercially-sensitive secrets from Western multinational firms. Finally, the new Decision names a North Korean firm for a number of cyber-attacks in Poland.[91]

(d) Cyberdefence

Cyberdefence is still underdeveloped in comparison to the economic and criminal law aspects of cybersecurity discussed above; it is still characterised by a piecemeal approach. As Odermatt rightfully states: 'there is no comprehensive EU approach to cyberdefence',[92] despite the claim that 'the next war will begin in cyberspace'.[93] The EU has slowly started to realize this and in 2014 adopted the first EU Cyber Defence Policy Framework, with a most recent update in 2018.[94] This document now clearly views cybersecurity as an integral part of the Union's defence strategy: 'Cyberspace is the fifth domain of operations, alongside the domains of land, sea, air, and space: the successful implementation of EU missions and operations is increasingly dependent on uninterrupted access to a secure cyberspace, and thus requires robust and resilient cyber operational capabilities.'[95] The document provides a framework for countering cyber threats and defines the cyberdefence aspects of the EU Cyber Security Strategy mentioned earlier. Its aim is to link cyberdefence issues to the Union's CSDP and maps the various steps to be take, together with the European Defence Agency (EDA). A good example of this is also to be found in the fact that cyberdefence has also become part of the PESCO framework, in which EU Member States work closely together in various projects. A number of these projects specifically focus on cybersecurity, including 'Cyber Threats and Incident Response Information Sharing Platform' and 'Cyber Rapid Response Teams and Mutual Assistance in Cyber Security'.[96]

To what extent could a cyber-attack trigger the common defence obligations EU Member States have on the basis of the Treaties? To answer that question, it is first of all important to note that the above-mentioned Cybersecurity Strategy refers to the so-called 'solidarity

---

[89] Art 4 of the Decision.

[90] Art 5 of the Decision.

[91] Council Decision (CFSP) 2020/1127 of 30 July 2020, OJ 246/12, 30.7.2020.

[92] Odermatt (n 9).

[93] General Keith B Alexander, upon accepting the post to lead the first United States Cyber-Command (USCYBERCOM). Quoted by Rex Hughes, 'A Treaty for Cyberspace' (2010) 86 *International Affairs* 523.

[94] Cyber Defence Policy Framework; https://www.consilium.europa.eu/media/37024/st14413-en18.pdf.

[95] Ibid.

[96] https://pesco.europa.eu/. See also Lorenzo Pupillo, Melissa K. Griffith, Steven Blockmans, Andrea Renda, 'Strengthening the EU's Cyber Defence Capabilities' (November 2018) *CEPS Report*.

clause' laid down in Article 222 TFEU.[97] On the basis of that provision obligations exists for the Union and its Member States to combine their efforts:

> The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States, to:
>
> (a)
>
> - prevent the terrorist threat in the territory of the Member States;
> - protect democratic institutions and the civilian population from any terrorist attack;
> - assist a Member State in its territory, at the request of its political authorities, in the event of a terrorist attack;
>
> (b) assist a Member State in its territory, at the request of its political authorities, in the event of a natural or man-made disaster.

Indeed, cyber-attacks are not mentioned explicitly. Yet, they easily fit under some of the headings. In a 2012 Resolution, the European Parliament even explicitly mentioned cybersecurity as falling within the scope of the solidarity clause: it called for 'an adequate balance between flexibility and consistency as regards the types of attacks and disasters for which the clause may be triggered, so as to ensure that no significant threats, such as attacks in cyberspace, pandemics, or energy shortages, are overlooked'.[98] In fact, the European Parliament even went a step further and also mentioned cyber-attacks as a reason to invoke the so-called 'mutual defence clause' laid down in Article 42(7) TEU, containing a provision comparable to Article 5 of the NATO Treaty:

> If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States.

The European Parliament took the view 'that even non-armed attacks, for instance cyberattacks against critical infrastructure, that are launched with the aim of causing severe damage and disruption to a Member State and are identified as coming from an external entity could qualify for being covered by the clause, if the Member State's security is significantly threatened by its consequences, while fully respecting the principle of proportionality'.[99] While in the case of the solidarity clause it may be argued that there needs to be a link with 'terrorism', the mutual defence clause refers to 'armed aggression', which in international law terms may rule out certain cyberattacks.[100] Hence, in both cases the application of the clauses to situations

---

[97] See for instance Yuri Bogmann-Prebil and Malcolm Ross (eds), *Promoting Solidarity in the European Union* (OUP 2010).

[98] European Parliament resolution of 22 November 2012 on the EU's mutual defence and solidarity clauses: political and operational dimensions (2012/2223(INI)) para 20.

[99] Ibid., para 13.

[100] *Cf* Roscini (Ch 14 of this Handbook) and Focarelli (Ch 15 of this Handbook).

of cybersecurity is not always obvious. In practice, however, invoking a solidarity or a mutual defence clause will most probably be driven more by political incentives than by legal doctrinal analysis.

4. CONCLUSION AND ASSESSMENT

The various hard and soft law instruments to regulate cybersecurity reveal that cyberspace has clearly become part of the EU's agenda and that a sub-discipline of 'EU Cybersecurity Law' is indeed in a nascent state. The relatively slow development of this area is not only related to the absence of clear legal competences on the side of the EU, but also to the early notion that by its very nature 'cyberspace' could and should not be regulated. It could not be regulated because of the fact that the phenomenon sits uneasily with traditional notions of territorial jurisdiction and it should not be regulated because 'regulatory efforts […] would unduly restrict the great potential of the Internet'.[101]

Over the years, however, the EU has put great efforts in formulating ambitious cybersecurity policies. While this has resulted in an impressive pile of policy and strategy papers produced by the various EU institutions (the Commission in particular), clear legal competences to actually regulate the field are indeed hard to find and measures do not necessarily relate to traditional notions of 'security'. As also rightfully held by others, 'Most of the EU's action in the field of cybersecurity has dealt with internal EU policies (e.g., internal market and consumer protection) or is linked to criminal law (combating cybercrime) and is tied to the goals of economic growth and the internal market'.[102] The focus on the social-economic dimension, is understandable since in that area connections were easier to make and the internal market still forms the core of what the EU stands for. In the words of Dewar: 'The system of exclusive, shared, supporting and special competences established a policy framework in which the EU was restricted to non-military, socio-economic policy choices. The result of this restriction was that only socio-economic considerations in cybersecurity could be developed and implemented.'[103] This also led to path dependencies and made it more difficult to connect to newer policy areas.[104]

At the same time, the EU now seems to be moving beyond internal measures only. In line with the more general increased attention for its global role,[105] the EU is clearly attempting to mainstream cyber issues throughout its existing foreign and security policy. One reason is that it is increasingly difficult to separate internal and external threats in this field.[106] The more active role of the EU in global debates and the recent initiatives on the 'cyber diplomacy

---

[101] Joachim Zekoll, 'Jurisdiction in Cyberspace' in Gunther Handl, Joachim Zekoll and Peer Zumbansen, *Beyond Territoriality: Transnational Legal Authority in an Age of Globalization* (Brill 2012) 342–43.

[102] Odermatt (n 9).

[103] Robert Scott Dewar, *Cyber Security in the European Union*, PhD thesis University of Glasgow, at 212.

[104] See on the incremental approach of the Union's in the regulation of cybersecurity also George Christou, 'The Collective Securitisation of Cyberspace in the European Union' (2019) 42 *West European Politics* 278.

[105] See for a recent assessment Wessel and Larik (n 35).

[106] Bendiek and Porter (n 25) 156–7.

toolbox' and restrictive measures against persons involved in cyber-attacks, reveal that the EU has been able to use existing competences in various *offline* fields, to regulate *online* activities.

Using various competences and different policy fields does, however, come at a price. This chapter points to the need for a comprehensive regulatory approach to overcome the current fragmentation in EU cybersecurity instruments. This fragmentation is not a choice, but simply results from the fact that no express cybersecurity competence exists and that it is not always easy (and sometimes even impossible) to combine the different cybersecurity dimensions in consistent or even connected policies due to the need for different legal bases. As held by some observers, 'one of the key challenges of cybersecurity regulation is to impose the right obligations on the right actors, through the right instrument'.[107] Even the field of 'security' is still characterized by a substantial degree of fragmentation, with security aspects being covered by the Internal Market, the Area of Freedom, Security and Justice (AFSJ) and the Common Foreign, Security and Defence Policy. Maintaining (or in fact creating) consistency (or at least coherence) in EU cybersecurity policy might very well be the main challenge for the EU the coming years.[108]

---

[107] Fuster and Jasmontaite (n 8) 109.

[108] See also Helen Carrapico and André Barrinha, 'The EU as a Coherent (Cyber)Security Actor?' (2017) 55 *JCMS* 1254, 1267:

> the EU has an explicit ambition to be a coherent security actor. However, both the architecture put in place under the [EU Cybersecurity Strategy] and the resistance from Member States to allow the EU to have a more stringent control over their cyber activities, limit the EU's coherence in the field. That said, both the rising political importance given to cybersecurity and the progressive consolidation of what is still a rather recent field of activity, means there are signs the EU might move towards a more coherent actorness in the field.

24. NATO and the international law of cyber defence

Steven Hill[1]

1. INTRODUCTION

The North Atlantic Treaty Organization (NATO) is a political-military alliance composed of 30 Allies.[2] Its mandate is to address a wide range of current and emerging challenges affecting international security. For more than two decades, this has included security challenges related to cyberspace.

In 2019, NATO celebrated an important milestone with the 70th anniversary of the entry into force of the Alliance's foundational instrument, the North Atlantic Treaty. That anniversary generated a series of reflections[3] about how NATO has adapted to an evolving security environment in line with the core values of democracy, individual liberty, and the rule of law set forth in its founding document, the 1949 North Atlantic Treaty.[4]

In line with this commitment to the rule of law, NATO has also been explicit about the role of international law in its cyber defence policy. For example, it has consistently reaffirmed the applicability of international law in cyberspace and stated that the alliance will act in accordance with international law and the principle of restraint. NATO also sees itself as supporting – and ultimately benefitting from – a norms-based, predictable and secure cyberspace.

This chapter seeks to describe the current State of NATO's work in the field of cyber defence and to assess how this work relates to broader debates on international law as it applies to cyberspace. First, it describes the cyber threat environment as currently perceived in the Alliance. Then it provides a brief historical overview of the evolution of NATO cyber policy and the development of NATO structures, with an emphasis on developments since 2014. Finally, it highlights some the international law considerations that have risen in this evolution. In doing so, it suggests some insights that NATO's experience might have for the broader field of international law as it applies to cyberspace. It also suggests some ways in which NATO can continue to encourage the development of this field.

---

[1] This chapter reflects the author's personal views and does not represent those of NATO or its Allies. The author would like to thank Nadia Marsan, Massimo Signoretti, and Chelsey Slack for their comments and suggestions. All websites were last accessed on 13 November 2020.

[2] The Republic of North Macedonia deposited its instrument of ratification of the North Atlantic Treaty on 27 March 2020, thus becoming the thirtieth NATO Ally. NATO also cooperates with a wide range of partners in Europe, the Middle East and North Africa, and around the globe.

[3] See the description of some of these events in Steven Hill, 'NATO at 70—The NATO Legal Community's Contribution' (2019) 34 *Emory Int'l L Rev* 1.

[4] *North Atlantic Treaty*, 4 April 1949, 34 U.N.T.S. 243, Preamble.

2. NATO'S CYBER THREAT ENVIRONMENT

The years since the publication of the first edition of this *Research Handbook* in 2015 have seen considerable evolution in cyber threats to NATO and individual Allies.[5] At their 2018 summit in Brussels, Allied Heads of State and Government recognised that these threats 'are becoming more frequent, complex, destructive and coercive'. They are often a component of broader hybrid threats, which 'combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces'.[6]

In a public speech at France's École Militaire in May 2018, NATO Secretary General Stoltenberg described the threat environment against NATO Allies:

> Here in France, TV-Cinq Monde was taken off air by hackers. 'Fancy Bear', a group associated with the Kremlin, hacked the main political parties in the United States in a brazen attempt to influence the 2016 election. Last years' WannaCry attack forced Renault to halt production at several of its factories. And brought hospitals in the United Kingdom to a standstill. The very nature of these attacks is a challenge. It is often difficult to know who has attacked you. Or even if you have been attacked at all. There are many different actors. Governments, but also criminal gangs, terrorist groups and lone individuals. Nowhere is the 'Fog of War' thicker than it is in cyberspace. Low cost and high impact, cyber-attacks are now a part of our lives. Some seek to damage or destroy. If these were hard attacks, using bombs or missiles instead of computer code, they could be considered an act of war. But instead, some are using software to wage a soft-war.[7]

It is also useful to consider the impact of this threat environment on NATO's own networks, which cover over 60 different locations including NATO operations in the field. According to published information, these have been increasingly targeted: 'NATO cyber defence systems register suspicious events each day: from low-level attempts to technologically sophisticated attacks against NATO networks.'[8]

Given this threat environment,[9] it is not surprising that bolstering cyber defences has taken on increasing visibility in recent years. Moreover, the cyber threat environment will continue to evolve in years to come, including with the development of new technologies. NATO

---

[5] This chapter seeks to update Dr Katharina Ziolkowski's excellent account of NATO's cyber defence policy in the first edition. Katharina Ziolkowski, 'NATO and Cyber Defence' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook of International Law and Cyberspace* (Edward Elgar 2015). While its descriptions of many aspects of NATO's cyber defence policy remain accurate and useful, this work was finalised in 2013 and does not take into account major developments since then. These developments will be the focus of this chapter.

[6] See NATO, 'NATO's Response to Hybrid Threats,' https://www.nato.int/cps/en/natohq/topics_156338.htm.

[7] 'Speech by Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference', Ecole Militaire Speech (15 May 2018) https://www.nato.int/cps/en/natohq/opinions_154462.htm.

[8] 'NATO Cyber Defence', https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf.

[9] For an overall synthesis of the current threat environment and its implications for NATO policy, see generally Antonio Missiroli, 'The Dark Side of the Web: Cyber as a Threat' (2019) 24 *European Foreign Affairs Review* 135.

remains focused on ensuring that its cyber defences remain fit-for-purpose for the future.[10] As the Heads of State and Government put it when they met in London in December 2019:

> [t]o stay secure, we must look to the future together. We are addressing the breadth and scale of new technologies to maintain our technological edge, while preserving our values and norms….We are increasing our tools to respond to cyber attacks, and strengthening our ability to prepare for, deter, and defend against hybrid tactics that seek to undermine our security and societies.[11]

3. NATO'S CYBER POLICY EVOLUTION: PAST, PRESENT AND FUTURE

NATO's policy on cyber defence has developed over the years in response to the evolution of the cyber threat landscape. This section begins with a discussion of the principal actors in cyber policy development and implementation within NATO. It then provides a historical account of the development of NATO cyber policy from 2002 to 2020.

(a) Principal Actors

All decisions within NATO are taken by consensus of all Allies. Cyber defence policy is implemented by NATO's political, military and technical authorities, as well as by individual Allies.[12] This section seeks to provide a broad overview of the different stakeholders involved in cyber defence policy and implementation.[13]

In terms of intergovernmental bodies, the North Atlantic Council (NAC), NATO's supreme governing body composed of representatives of all Allies, is the ultimate high-level political oversight over cyber defence policy and the apex of NATO's cyber defence governance. At the working level under the NAC, the Cyber Defence Committee (CDC) is staffed by cyber policy experts – and, increasingly, an emerging core of dedicated 'cyber diplomats' – from each Ally. It meets on a regular basis, at times several times per week.[14] The CDC's role includes preparing cyber policy drafts, reports, and other documents to be approved by the NAC. The NAC meets at least once weekly at the ambassadorial level, three times per year at the level of Ministers of Foreign Affairs, three times per year at the level of Ministers of Defence, and once approximately every two years at the level of Heads of State and Government. These high-level meetings often include dedicated sessions or briefings dedicated to cyber policy. NATO's major cyber defence policies and decisions have been approved in the summits of Heads of State and Government.

---

[10] 'NATO Staying Strong in Cyberspace' (24 March 2020) https://www.nato.int/cps/en/natohq/news_174499.htm?selectedLocale=en.

[11] 'London Declaration' (4 December 2019) https://www.nato.int/cps/en/natohq/official_texts_171584.htm, paras 5-6.

[12] NATO, 'Cyber Defence', https://www.nato.int/cps/en/natohq/topics_78170.htm.

[13] For further information about the background of NATO's current cyber governance structures, see the more detailed descriptions at Ziolkowski (n 5) and David P Fidler, Richard Pregent and Alex Vandurme, 'NATO, Cyber Defence, and International Law' (2013) 4 *St. John's Journal of International and Comparative Law* 1.

[14] In addition to the CDC, the NATO Consultation, Control and Command (NC3) Board is a forum for intergovernmental consultation on technical and implementation aspects of cyber defence.

As part of NATO's alliance-level structures, a team of international civil servants based in the Emerging Security Challenges Division of NATO's International Staff provides staff support to all of these discussions. The International Staff also coordinates the contributions of other parts of the NATO system to intergovernmental discussions. The NATO Military Authorities (NMA) and the NATO Communications and Information Agency (NCIA) bear the specific responsibilities for identifying the statement of operational requirements, acquisition, implementation and operating of NATO's cyber defence capabilities. Allied Command Transformation (ACT) has the lead for setting the requirements for capability development as well as education and training activities such as the annual Cyber Coalition Exercise. Given the many actors involved in cyber defence throughout the NATO system, there is a need for a forum to provide leadership and guidance, including in crises. This is the role played by the Cyber Defence Management Board, a senior body composed of stakeholders across the NATO system that is convened to discuss and coordinate activities on a wide range of cyber defence issues.

Although it is not a NATO body like the others mentioned above, it is worth highlighting the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) located in Tallinn, Estonia. This is a NATO-accredited centre that currently has 25 member nations, including both NATO Allies and partners. Its mission is to support these nations and NATO 'with unique interdisciplinary expertise in the field of cyber defence research, training and exercises covering the focus areas of technology, strategy and law'.[15] From the perspective of the vast world outside the halls of NATO, the Alliance's most visible contribution to international law is almost certainly the two editions of the *Tallinn Manual on the International Law Applicable to Cyber Operations*. Produced by groups of independent experts convened by the CCDCOE, these two commentaries do not represent official NATO doctrine. They have received wide attention in the cyber community and been influential in shaping international debate. In some areas, they have also spurred a considerable amount of useful debate that has helped States clarify their positions.

Finally, outside alliance structures, NATO also cooperates with a wide range of other stakeholders. This involves building networks with officials responsible for cyber defence issues in countries outside the alliance as well as in other international organisations and the European Union.[16] NATO also works closely with academics and with the private sector.[17] One example of private sector cooperation is the Malware Information Sharing Platform, launched in 2013. This platform includes both governments and private sector companies and 'facilitates information sharing about the technical characteristics of malware within a trusted community'.[18]

---

[15] See CCDCOE, 'About Us', https://ccdcoe.org/about-us/.

[16] For more detail on NATO's partnerships in the cyber defence area, see Neil Robinson and Chelsey Slack, 'Co-operation: A Key to NATO's Cyberspace Endeavour' (2019) 24 *European Foreign Affairs Review* 153.

[17] Ibid.

[18] 'Sharing Malware Information to Defeat Cyber Attacks' (29 November 2013) https://www.nato.int/cps/en/natolive/news_105485.htm.

(b) Development of NATO Cyber Defence Policy

This section provides a historical account of the development of NATO cyber policy from 2002 to 2020. Major steps in cyber defence policy have generally been adopted or endorsed at NATO summits. Moreover, as one observer has observed, '[o]fficial commitments made at NATO summits on cyber security have become increasingly granular'.[19] This section follows the usual practice of describing policy development by reference to these milestones, even though this summit-to-summit trajectory risks presenting the evolution of NATO's policy as foregone conclusion. Like all decision making at the diplomatic level, NATO policy is also related to the broader political context as well as the need to maintain consensus-based decision making.

When considering the evolution of NATO's policy, it is important to keep in mind certain core elements that have remained constant over the years. One constant is the basic allocation of responsibility between the defence of NATO's own networks and the defence of national networks. NATO is responsible for the defence of its own networks. NATO does have some capability to respond to requests for assistance by individual Allies. However, the general rule is that Allies are responsible for the defence of their own networks. This in line with the requirements of Article 3 of the North Atlantic Treaty.[20] Another constant is the defensive nature of NATO policy. In line with this defensive mandate, NATO as an organization does not possess or seek to develop offensive cyber capabilities.

(i) From Prague to Chicago 2002–2012

The initial focus of the alliance's approach was largely technical in nature. As time passed and cyber elements became more central to military operations, cyber defence issues began to be considered at the policy and eventually the political level. In 2002, the NATO Computer Incident Response Capability (NCIRC) was established to protect NATO's networks, an important step in provide some baseline technical means to defend NATO networks. The brief reference in the 2002 Prague Summit declaration to the need to 'strengthen our capabilities to defend against cyber attacks' was the first mention of cyber issues in a NATO document agreed at the Head of State or Government level.[21]

The 2007 cyber attacks on Estonian public and private institutions were a turning point that prompted NATO to take a harder look at cyber defence. In particular, this meant conceiving of cyber defence challenges as not just as a technical issue. Rather, 'the need for a policy and doctrine became apparent and cyber defence entered the political arena of the Alliance'.[22] As a result of this shift, NATO adopted its first cyber defence policy in the lead up to its NATO

---

[19] Max Smeets, 'NATO's Cyber Policy 2002-2019: A very, very brief overview' (2 December 2019) http://maxsmeets.com/2019/12/natos-cyber-policy-between-2002-2019-a-very-very-brief-overview/.

[20] North Atlantic Treaty, art 3, 'In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack'.

[21] 'Prague Summit Declaration' (21 November 2002) https://www.nato.int/cps/en/natohq/official_texts_19552.htm.

[22] Ziolkowski (n 5) 429.

Summit in Bucharest in 2008.[23] This policy established the objectives, principles and organisational elements related to NATO cyber defence.

The cyber strategic environment changed again in the summer of 2008 when Russia's actions against Georgia highlighted the emerging role of cyber attacks as integral components of Russia's military operations. As a reflection of this heightened sense of the link between international security and cyber attacks, the NATO Strategic Concept adopted at the Lisbon Summit in 2010 recognised that 'cyber attacks…can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability'.[24]

This recognition spurred the development of a new NATO cyber defence policy in 2011, which continued to prioritise the protection of NATO's own networks. This time the focus was on further centralising the protection of these networks within the NATO enterprise. At the same time, the policy provided for the use of the NATO Defence Planning Process (NDPP) to enhance national cyber defences of Allies through the development of cyber defence capability targets for each Ally, including regular monitoring of each Ally's progress toward meeting these targets. The NDPP is 'a framework within which Allies harmonise their national defence plans with those of NATO, without compromising their national sovereignty'.[25] At the same time, the decision to extend the NDPP to national cyber capabilities was significant because it represented a shift of emphasis: while NATO's focus was formally still on the defence of its own networks, it would also begin focus on building resilience of Allies. This shift was based on the notion that in matters of cyber defence, the alliance is only as strong as its weakest link.

(ii) Wales 2014

By 2014, when Russia began to use cyber attacks as part of its sophisticated hybrid warfare operations against Ukraine, the threat environment had once again evolved to the point where another update to NATO policy was needed.[26] It was at the Wales Summit in 2014 that Heads of State and Government approved the Enhanced Cyber Defence Policy. This policy is still in force.

While the policy itself has not been publicly released, its key elements are described in the declaration adopted at the Wales Summit in September 2014.[27] These included several decisions that are relevant to Allies' perception of the international law related to cyberspace. First, Allies acknowledged that the impact of cyber attacks 'could be as harmful to modern societies as a conventional attack'.[28] They affirmed that 'cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation

---

[23] 'Bucharest Summit Declaration' (3 April 2008) https://www.nato.int/cps/en/natolive/official_texts_8443.htm.

[24] 'NATO Strategic Concept' (2010) https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf.

[25] For more information on the NDPP, see 'NATO Defence Planning Process', https://www.nato.int/cps/en/natohq/topics_49202.htm.

[26] On the emerging need to adapt to the new threat environment, see Matthijs Veenendaal, Kadri Kaska and Pascal Brangetto, 'Is NATO Ready to Cross the Rubicon on Cyber Defence?' (2016) https://ccdcoe.org/library/publications/is-nato-ready-to-cross-the-rubicon-on-cyber-defence/.

[27] 'Wales Summit Declaration' (5 September 2014) paras 72 and 73 https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[28] Ibid., para 72.

of Article 5 would be taken by the North Atlantic Council on a case-by-case basis'.[29] Second, Allies recognised that 'international law, including international humanitarian law and the UN Charter, applies in cyberspace'.[30] Third, Allies 'committed to developing further our national cyber defence capabilities, and we will enhance the cyber security of national networks upon which NATO depends for its core tasks, in order to help make the Alliance resilient and fully protected'.[31] Finally, a number of activities were expanded, including in the fields of cooperation with industry and other partner nations and international organisations, training, education, exercises and information sharing.[32]

(iii) Warsaw 2016

Two decisions from NATO's summit in Warsaw in 2016 stand out as significant milestones. The first major decision was that Allies recognised cyberspace 'as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea'.[33] The concept of 'domain of operations' is a military one. Recognising cyberspace as such a domain implies the need for increased level of capabilities to operate in that domain as well as for the accompanying military support structure, potentially including legal doctrine and training.[34] From a legal perspective, this decision also implies further Allied recognition that the general body of international law applying to the air, land and sea domains also applies in cyberspace, even if there may be specificities to the way general international law applies in this context. The second major decision from Warsaw was the adoption of a Cyber Defence Pledge.[35] The purpose of this pledge is to strengthen and enhance the cyber defences of their national networks and infrastructures as a matter of priority. While the pledge is not legally binding, Allies do submit periodic reports on its implementation. These are considered at annual conferences.

In addition to these two cyber policy decisions taken at the Warsaw Summit itself, on the margins of the meeting, the NATO Secretary General Stoltenberg, European Council President Tusk, and European Commission President Juncker signed a joint declaration committing to enhanced cooperation between NATO and the European Union in a wide range of fields, including more 'coordination on cyber security and defence including in the context of our missions and operations, exercises and on education and training'. [36] This is one example

---

[29] Ibid.

[30] Ibid.

[31] Ibid., para 74.

[32] Ibid.

[33] 'Warsaw Summit Communiqué' (9 July 2016) para 70, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[34] For additional analysis of this decision, see Tomáš Minárik, 'NATO Recognises Cyberspace as a "Domain of Operations" at Warsaw Summit', https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/.

[35] 'Cyber Defence Pledge' (8 July 2016) https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

[36] 'Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization' (8 July 2016) https://www.nato.int/cps/en/natohq/official_texts_133163.htm. For more details on the joint measures in implementation of this joint declaration, see Lorena Trinberg, 'EU-NATO Relations: Hand In Hand Against Cyberattacks' (2017) https://ccdcoe.org/incyder-articles/eu-nato-relations-hand-in-hand-against-cyberattacks/.

of NATO's ongoing cooperation with a wide range partner nations and international organisations on cyber issues.

(iv) Brussels 2018 and beyond

The period between the 2016 Warsaw and NATO's next summit at its new headquarters in Brussels in 2018 would be devoted largely to the implementation of the decision to recognise cyberspace as a domain of operations through a series of new doctrinal documents as well as organizational challenges.[37] This work included a 'Military Vision and Strategy on Cyberspace as a Domain of Operations' and continuing work on NATO's first doctrine for military cyber operations.[38] That doctrine was adopted in January 2020.[39] At the Brussels summit, Allies further agreed to establish a new Cyberspace Operations Centre as part of NATO's strengthened command structure at the summit in July 2018. That facility has opened under the command of the Supreme Commander Allied Forces Europe (SACEUR)[40] and will reportedly be fully operational by 2023.[41]

One significant decision taken in Brussels was to enable NATO to draw on national cyber capabilities for its missions and operations. This required a delicate balance between the traditional defensive orientation of NATO's policy and the notion that operating in the military domain of operations of cyberspace might require more than just a narrow range of defensive actions.[42] Rather than authorise a departure from NATO's defensive mandate and a move into offensive cyber capabilities for the alliance, Allies announced agreement on 'how to integrate sovereign cyber effects, provided voluntarily by Allies, into Alliance operations and missions, in the framework of strong political oversight'.[43] This will be done in a way that fully respects the defensive mandate.[44] To date, a number of allies have announced that they will contribute

---

[37] For an assessment of the overall state of NATO's cyber work following the Brussels summit, including the implementation of the domain of operations decision, see Laura Brent, 'NATO's Role in Cyber', *NATO Review* (12 February 2019) https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html. See also Jamie Shea, 'Cyberspace as a Domain of Operations: What Is NATO's Vision and Strategy?' (2018) 9 *MCU Journal* 133.

[38] See Brent, ibid.

[39] See 'Allied Joint Doctrine for Cyberspace Operations', Allied Joint Publication AJP-3.20, Edition A, Version 1, (January 2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

[40] See 'Opening Remarks by Air Chief Marshal Sir Stuart Peach, Chairman of the NATO Military Committee at the 182nd Military Committee in Chiefs of Defence Session' (14 January 2020) https://www.nato.int/cps/en/natohq/opinions_172482.htm?selectedLocale=en.

[41] See Robin Emmott, 'NATO cyber command to be fully operational in 2023', *Reuters* (16 October 2018) https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9.

[42] See Max Smeets, 'NATO Allies Need to Come to Terms With Offensive Cyber Operations' (14 October 2019) *Lawfare*, describing:

> an uneasy situation within cyber cooperation: Allies do not agree on the appropriate procedures and boundaries for offensive cyber operations. More specifically, there is no agreement on when military cyber organizations can gain access to systems and networks in allied territory to disrupt adversarial activity ... this issue may end up causing significant loss in allies' trust and confidence.

[43] See 'Brussels Summit Declaration' (11 July 2018) https://www.nato.int/cps/en/natohq/official_texts_156624.htm, para 20.

[44] Outside commentary suggests that consensus on this issue took considerable work to achieve. See, e.g., Massimiliano Signoretti, 'Cyber Defence at the 28th NATO Summit in Brussels, 11-12 July 2018',

sovereign cyber effects to support NATO missions.[45] The details of how this integration is to be done have not been released publicly.

The Brussels summit declaration also includes language that helps understand how NATO's core mission of deterrence and defence works with respect to cyber threats. First, the Heads of State and Government declared that 'we are determined to employ the full range of capabilities, including cyber, to deter, defend against, and to counter the full spectrum of cyber threats, including those conducted as part of a hybrid campaign'.[46] This means that NATO reserves the right to defend against cyber attacks using all means available at its disposal, in accordance with international law.

Second, they highlighted the 'need to bolster our intelligence-led situational awareness to support NATO's decision-making and action'.[47] Information sharing, either among allies, with the EU, or with industry has been a consistent feature of NATO's cyber policy over the years. NATO is making considerable efforts to achieve better overall intelligence sharing and coordination, including through establishing a new Joint Intelligence and Security Division.[48] The demand for intelligence sharing, including in the cyber area, will certainly increase in the future. This may make existing difference of legal approach among allies, particularly on either side of the Atlantic, starker.[49]

Third, allied leaders emphasise another aspect of deterrence and defence, namely continuing to 'work together to develop measures which would enable us to impose costs on those who harm us'.[50] In February 2019, Allies endorsed 'a NATO guide that sets out a number of tools to further strengthen NATO's ability to respond to significant malicious cyber activities'.[51] The details of these measures have not been released, but they aim to 'help NATO and its Allies to enhance their situational awareness about what is happening in cyberspace, boost their resilience, and work together with partners to deter, defend against and counter the full spectrum

---

https://ccdcoe.org/incyder-articles/cyber-defence-at-the-28th-nato-summit-in-brussels-11-12-july-2018/:

> the wording seems to reveal that the discussion on the topic (integration of 'sovereign cyber effects') might have been a complex one, with Allies striving to reach a common understanding. The need to affirm that political oversight of the entire process would be particularly intense ('strong political oversight'), might suggest that sensitive matters were at stake, and that Allies may have had sharply differing views regarding the potential conduct of cyber operations.

[45] See Piret Pernik, 'National Cyber Commands' in Eneken Tikk and Mika Kerttunen, *Routledge Handbook of International Cybersecurity* (Routledge 2020), citing five allies, Estonia, Denmark, the Netherlands, the UK, and the US. See also Shannon Vavra, 'NATO Cyber-operations Center will be Leaning on its Members for Offensive Hacks' (30 August 2019) https://www.cyberscoop.com/nato-cyber-operations-offensive-hacking-neal-dewar/ (referring to nine allies). The number of allies offering to make their own effects available to the alliance will likely increase over time.

[46] Brussels Summit Declaration (n 43) para 20.

[47] Ibid.

[48] For more background, see Arndt Freytag von Loringhoven, 'A New Era in NATO Intelligence', *NATO Review* (29 October 2019) https://www.nato.int/docu/review/articles/2019/10/29/a-new-era-for-nato-intelligence/index.html.

[49] *See* Steven Hill, *Transatlantic Interoperability Challenges in the Law of Armed Conflict in 2040*, Lieber Institute for Law and Land Warfare, United States Military Academy (forthcoming 2020) (citing transatlantic differences over data as a strategic-level challenge)

[50] Brussels Summit Declaration (n 43) para 20.

[51] NATO Cyber Defence (n 8).

of cyber threats'.[52] This set of tools was meant to complement the measures in the EU's 'Cyber Diplomacy Toolbox',[53] which is a series of measures that form the framework for a joint EU diplomatic response to malicious cyber activities.[54]

Finally, NATO's response to the COVID-19 pandemic has had a cyber defence element, focusing on the need to bolter national cyber defence in order to respond to the increase in malicious cyber activities that accompanied the pandemic. The North Atlantic Council addressed cyber threats against sectors involved with the pandemic recovery. In June 2020, it adopted a statement 'condemn[ing] destabilising and malicious cyber activities directed against those whose work is critical to the response against the pandemic, including healthcare services, hospitals and research institutes' and confirming that allies 'stand in solidarity with those who have been affected by malicious cyber activities and remain ready to assist Allies, including by continuing to share information, as they respond to cyber incidents that affect essential services'.[55]

4. INTERNATIONAL LAW AND NATO CYBER DEFENCE POLICY

What role has international law played in the evolution of NATO's cyber defence policy? And what influence might NATO's cyber policy decisions have on the international law applicable to cyberspace?

(a) Applicability of International Law to Cyberspace

Perhaps the most straightforward way in which international law has played a role in NATO's cyber policy evolution has been in the Alliance's constant affirmations of the applicability of international law in cyberspace. As explained above, at the NATO Summit in Wales in 2014, Allies recognised that international law, including international humanitarian law and the UN Charter, applies in cyberspace. More recently, at the Brussels Summit in July 2018, allies re-affirmed their commitment to act in accordance with international law, including the UN Charter, international humanitarian law, and human rights law, as applicable.

These statements were part of a broader movement of cyber diplomacy conducted by States, international organisations, and non-governmental organisations. That effort had some notable successes at the international level, including the 2013 and 2015 reports of the UN Group

---

[52] Ibid.

[53] See Council of the European Union, 'Cyber Attacks: EU Ready to Respond with a Range of Measures, including Sanctions' (19 June 2017) https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.

[54] For an assessment, see Katriina Härmä and Tomáš Minárik, 'European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox' (2017) https://ccdcoe.org/incyder-articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/.

[55] 'Statement by the North Atlantic Council Concerning Malicious Cyber Activities' (3 June 2020) https://www.nato.int/cps/en/natohq/official_texts_176136.htm?selectedLocale=en.

of Governmental Experts.[56] However, this consensus proved to be tenuous. Currently some States, among them China and Russia, are pushing back on the very notion of the applicability of international law principles, including the applicability of international humanitarian law, in cyberspace.[57] Many NATO Allies are attempting to counter these attempts to dismantle previous consensus. Their techniques include detailed legal statements of a series of how international law applies in cyberspace.[58] However, while the number of States making such statements is slowly growing, it still remains a small number that of course does not include all NATO allies. In this context, language like that adopted at NATO can be useful as evidence of where all NATO allies and likeminded States currently stand.[59] These and similar statements in other international organizations may help with ongoing cyber diplomacy.

(b) Article 5 and Armed Attack

International law considerations have also factored into NATO's cyber policy in relation to Article 5 of the North Atlantic Treaty. As mentioned above, the 2014 Wales Summit contained the basic policy decision regarding the interplay between cyber attacks and the international law concept of armed attack: 'We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis'. Article 5 is the self-defence provision at the core of the North Atlantic Treaty.[60] It refers back to Article 51 of the UN Charter, which itself reflects the 'inherent' right of self-defence under customary international law. In NATO's practice to date, Article 5 has been treated as coterminous with

---

[56] See UN General Assembly, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', 24 June 2013, UN Doc A/68/98, paras 19–20, https://undocs.org/A/68/98 and Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, para 28(b), https://undocs.org/A/70/174.

[57] See Michael N Schmitt and Liis Vihul, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms' (30 June 2017) *Just Security*, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

[58] For an overview of statements made by seven States (Australia, Estonia, France, Germany, the Netherlands, the UK, and the US), see Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views' (March 2020) https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views.

[59] See, e.g, Michael N Schmitt, 'Noteworthy Releases of International Cyber Law Positions – Part I: NATO' (27 August 2020) *Articles of War*, https://lieber.westpoint.edu/nato-release-international-cyber-law-positions-part-i.

[60] Article 5 reads:

> The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

the customary right reflected in Article 51.[61] All of these formulations revolve around the notion of armed attack.

From an international law perspective, NATO's policy illustrates at a minimum that a cyber attack *could* constitute an armed attack giving rise to the right of individual or collective self-defence under international law. It clearly does not say that *all* cyber attacks would rise to this level. Nor does it provide any further guidance on important international law questions, such as the threshold for an armed attack. For example, the policy does not refer to the well-known analysis that an armed attack must attain a certain level of scale and effect. That analysis features prominently in a range of judicial decisions[62] and in scholarly commentary.[63] Nor does it seek to address some of the debated questions. These include whether an attack 'having severe albeit neither injurious nor physically destructive effects could ever constitute an armed attack and, if so, under what circumstances'.[64]

From a policy perspective, the primary reason for this lack of detail about what would constitute an armed attack is straightforward. It is seen as strengthening the deterrence value of NATO's posture. The NATO Secretary General has said: 'I am often asked, "under what circumstances would NATO trigger Article 5 in the case of a cyber-attack?" My answer is: we will see. The level of cyber-attack that would provoke a response must remain purposefully vague'.[65] In any event, as the policy makes clear, the decision to invoke Article 5 would be taken on a case-by-case basis. This decision would be taken by the North Atlantic Council on the basis of consensus of all Allies. Whether or not an armed attack has occurred is a question of fact and law. NATO does not prejudge the threshold for an Article 5 decision. This would be a political decision in which a wide range of factors, including but not limited to legal advice, would be considered by the North Atlantic Council.

If Article 5 were invoked in response to a cyber attack, the Alliance's collective response would also be decided on a case-by-case basis by the North Atlantic Council. The legal obligation on Allies under Article 5 is set forth in the North Atlantic Treaty:

> each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.[66]

---

[61] See Aurel Sari, 'The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats' (2019) 10 *Harvard Nat'l Sec. J.* 405. See also Michael N Schmitt, 'The North Atlantic Alliance and Collective Defense at 70: Confession and Response Revisited' (2019) 34 *Emory Int'l L. Rev* 85. On self-defence in cyberspace see Focarelli (Ch 15 of this Handbook).

[62] See, e.g., *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. USA)*, Judgment [1986] ICJ Rep 14, para 195.

[63] For an exhaustive analysis of the concept of armed attack and its interpretation under the UN Charter, see Tom Ruys, *Article 51 and 'Armed Attack' and Article 51 of the UN Charter* (CUP 2011). For a cyber-specific analysis, see Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) Rule 71 and accompanying commentary.

[64] Schmitt (n 61), asking 'may a State treat a cyber operation that causes widespread and severe disruption to its economic system as an armed attack? Or do hostile cyber operations that seriously interfere with the functioning of critical cyber infrastructure qualify as such if the interference has not caused injury or physical damage?'.

[65] Ecole Militaire Speech (n 7).

[66] Article 5 further provides that '[a]ny such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the

This is an obligation of assistance to the State or States that are the victim of the armed attack. The Treaty does not specify what actions the attacked State's Allies are under an obligation to take. Rather, it requires each Ally to take 'such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area'. The text specifies that this is actions for all each ally to take both on its own and together with ('in concert with') other Allies.

It is impossible to predict what might happen if NATO Allies were to decide that a future cyber attack crosses the armed attack threshold in Article 5. The exact collective response would be decided on a case-by-case basis by the North Atlantic Council. This could include the use of force in exercise of the right of individual or collective self-defence. Such a use of force would not necessarily be limited to the cyber domain and could include action in other domains. As Secretary General Stoltenberg put it, NATO's response under Article 5 'could include diplomatic and economic sanctions, cyber-responses, or even conventional forces, depending on the nature and consequences of the attack'.[67] Finally, given the text of Article 5, it is possible that in addition to the collective response agreed by consensus, individual States would take action that they deem appropriate.

(c) 'Below the Threshold' Incidents

Since the vast majority of cyber incidents occurs below the armed attack threshold, international lawyers have had to think about the peacetime legal framework for responses to such malicious cyber activity. NATO's recent work has included 'a NATO guide that sets out a number of tools to further strengthen NATO's ability to respond to significant malicious cyber activities'.[68] However, this is document is not publicly available, so it is difficult to assess what its contents may indicate on some of the key questions that arise in responding to internationally wrongful acts against the Alliance or individual Allies.

In response to future incidents, Allies may wish to use NATO as a forum to coordinate multilateral responses to such responses, or as a means of requesting assistance with their own responses. In the case of a serious incident, one option would be to request consultations under Article 4 of the North Atlantic Treaty. Article 4 provides that '[t]he Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened'. Article 4 has only been explicitly been called upon in a handful of situations during NATO's history, none of which has been focused on cyber.[69] It is certainly possible that future malicious cyber activity could constitute the kind of threat to territorial integrity, political independence or security envisioned by Article 4. However, it is not necessary to use Article 4 in order for NATO to take action to deal with any given incident.

Security Council has taken the measures necessary to restore and maintain international peace and security'.

[67] Ecole Militaire Speech (n 7).

[68] NATO Cyber Defence (n 8).

[69] See Ulf Häußler, 'Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty' in Kadri Kaska, Anna-Maria Tallihärm and Eneken Tikk, *International Cyber Security Legal & Policy Proceedings* (CCDCOE 2010), 'in discussions the fact that the North Atlantic Council discussed the 2007 cyber attack faced by Estonia has repeatedly been cited as an example of Article 4 consultations despite the fact that neither Estonia nor the Council as a whole mentioned this provision'.

Close attention to NATO's future responses to 'below the threshold' cyber incidents may yield some insight on a range of international law questions. For example, given NATO's collective defence mandate, one question is whether States will be willing to consider NATO as a means to conduct collective countermeasures. At the time of writing, some Allies appear to have different views on whether collective countermeasures are a legally available option under international law.[70]

Finally, some NATO allies have developed a practice of using public identification of the perpetrators of malicious cyber activity as a means of countering that activity. This practice is referred to as attribution. As the Brussels Summit declaration put it in 2018, '[i]ndividual Allies may consider, when appropriate, attributing malicious cyber activity and responding in a coordinated manner, recognising attribution is a sovereign national prerogative'.[71] There is an increased trend of States making attributions, either unilaterally or in concert with others.[72]

(d) Providing a Forum for Expressing Legal Views

As an international organisation, NATO does not create international law or other norms that regulate State behaviour. While NATO's cyber practice to date may help shed light on some questions of international law (or at least help stimulate thinking on these questions), there would be little appetite among Allies and in the broader international community for NATO to take a lead role in driving such debates forward.[73] Put another way, NATO does not see itself as a norm-creating institution. At the same time, as a well-established multinational intergovernmental organisation with a considerable amount of practical experience on cyber defence issues, NATO can often provide a good vantage point not just for emerging State practice, but for encouraging it to be expressed.

More and more States have been making public statements of their views of how international law applies in cyber space. This process should be encouraged. One of the advantages of NATO is that it provides a forum for daily multilateral discussions and exchanges of views on cyber defence. NATO is also a way for Allies that have not yet taken a view on a subject can express support or alignment with positions of other Allies. Regular meetings at the ministerial and even Head of State and Government level provide an opportunity for Allies to make clear public statements. In addition, NATO has the convening power to host regular high-level interaction between government cyber policy experts, lawyers, academics and industry representatives. Sometimes sponsored and led by individual Allies, these are initiatives that can take a holistic approach by bridging the legal, political, and military domains. Finally, NATO also conducts regular multilateral cyber exercises, often with a legal component or designed so

---

[70] See Przemysław Roguski, 'Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea?' in Taťána Jančárková, Lauri Lindström, Massimiliano Signoretti, Ihsan Tolga and Gábor Visky (eds), *12th International Conference on Cyber Conflict: 20/20 Vision: The Next Decade* (CCDCOE 2020).

[71] Brussels Summit Declaration (n 43) para 20.

[72] See generally Kristen E Eichensehr, 'The Law and Politics of Cyberattack Attribution' (2020) 67 *UCLA L. Rev.* 520 (describing State practice).

[73] See Steven Hill and Nadia Marsan, 'International Law in Cyberspace: Leveraging NATO's Multilateralism, Adaptation and Commitment to Cooperative Security' in Dennis Broeders and Bibi Van Den Berg (eds), *Governing Cyberspace Behavior, Power and Diplomacy* (Rowman and Littlefield 2020).

as to raise legal questions. Properly designed, multilateral cyber defence exercises that engage the highest level of government decision makers could help clarify State practice. Leveraging all of these advantages may help generate more clarity on the international legal framework.

5. CONCLUSION: FUTURE CHALLENGES FOR NATO CYBER DEFENCE POLICY

NATO's cyber policy evolution over more than two decades has been a prime example of how the Alliance has adapted to new threats. What challenges can NATO expect in future cyber policy? And how can NATO's traditional approach to legal issues pertaining to cyberspace help the alliance address these challenges? In the future, the trajectory for NATO's cyber defence policy work will continue to be shaped by the threat environment as it evolves and will likely follow the direction indicated by existing work as the alliance seeks to further strengthen the cyber defences of the alliance itself and those of individual allies, deter cyber activities directed against NATO and its allies, and respond to future incidents.

The future cyber threat environment will be equally if not more intense than NATO sees today. For example, cyber defence will need to become increasingly powered by artificial intelligence in order to respond to AI-powered attacks.[74] Especially as technology evolves, the cyber domain of operations will become more central to – and more integrated with – other domains. For example, in December 2019, NATO Heads of State and Government declared outer space as NATO's newest domain of operations.[75] There is a strong link between outer space and cyber.[76] If the intensity of attacks and their potential impact on all domains continues to increase, one future outcome would be for Allies to be interested in stronger responses to them. Whether Allies prefer to do this individually or on a bilateral or 'small group' basis, or whether they will seek out stronger collective tools for the alliance is an open question.

Given Allies' commitment to the rule of law, compliance with international law will continue to be a cornerstone of NATO's cyber policies in the future. The challenge will be how to ensure that other actors in the international system, both State and non-State, comply as well and whether the broad cooperation among like-minded States that has been developing in numerous venues can be sustained in the long term.[77] Pressure for more collective action against cyber attacks and malicious cyber activities may well raise the stakes on some of the open legal questions that have been on NATO's agenda. One recommendation would be for allies to continue their ongoing legal dialogue on questions such as the armed attack threshold for Article 5, the types of response measures available for malicious cyber activity below the armed attack threshold, whether techniques like countermeasures are available not just for use by an individual victim State but also for collective use, and others. Technological

---

[74] Can Kasapoglu and Baris Kirdemir, 'Artificial Intelligence and the Future of Conflict' in Tomás Valásek, New Perspectives on Shared Security: NATO's Next 70 Years (2019).

[75] See London Declaration (n 11) para 6.

[76] See Kestutis Paulauskas, 'Space: NATO's Final Frontier', *NATO Review* (13 March 2020), noting that 'cyber threats can impact on each of the segments [of satellite transmission of data] – software of the satellites, ground control, data links and the user'.

[77] See Chelsey Slack, 'Between a Rock and a Hard Place: Tempering National and International Tensions in Cyberspace' (2017) *CyFy Journal* 33, noting that 'despite the dense web of interdependence that characterises cyberspace, motivation for restraint and cooperation should not be taken for granted'.

developments may also lead to more calls for legal dialogue. For example, since applications of artificial intelligence and machine learning for use in cyber defence have already made their way onto NATO's agenda, there will likely be demand for multilateral ways of responding to them. Another recommendation would be for more dialogue on the legal framework for the use of such technologies.[78] Legal dialogue on these forward-looking issues might help bring allies closer together, not only in the legal area but in broader cyber policy terms.

[78] See Steven Hill, 'AI's Impact on Multilateral Military Cooperation: Experience from NATO' (2020) 114 *American Journal of International Law Unbound* 147, recommending multilateral dialogue on the legal aspects of emerging AI-powered military technologies. See also Nadia Marsan, 'AI and Machine Learning Symposium: Confronting Complexity through Collective Defence' (29 April 2020) *Opinio Juris*, http://opiniojuris.org/2020/04/29/ai-and-machine-learning-symposium-confronting-complexity-through-collective-defence/, suggesting that 'NATO can provide an excellent venue in which both Allies and Partners can collectively and pragmatically work to tackle and clarify the complexities and legal ambiguities arising from the use of AI/ML enabled military technology'.

25. Russian approaches to international law and cyberspace

Sergey Sayapin[1]

1. INTRODUCTION

Russia is a significant international actor in cyberspace. It has been accused of involvement in major cyber attacks affecting political and social processes in foreign States[2] and has itself been a victim of such attacks.[3] The intensifying activities of States and private actors in cyberspace have prompted Russia to develop domestic legislation pertaining to such activities, with the dual effect of reinforcing the protection of Russia's security interests, on the one hand, and letting the Russian State (and private actors acting in furtherance of the State's interests) operate relatively freely in cyberspace, on the other. Noticeably, a majority of Russia's domestic legal instruments pertaining to cyberspace do not refer to international law explicitly and, where they do, they imply the absence of relevant international law sources which further implies that ad hoc domestic regulations and solutions are preferable. This chapter offers an overview of Russia's approaches to the legal and institutional regulation of cyberspace, with a focus on the Constitution, relevant Federal Laws, Decrees issued by the President, as well as the applicable criminal and administrative law. The chapter also considers the scope of applicable international law rules by looking into relevant legislation and practice.

2. LEGISLATION

The Russian Federation's domestic legislation applicable to the regulation of cyberspace may be grouped under three headings: (1) relevant constitutional provisions; (2) laws and regulations dealing specifically with cyberspace issues; and (3) Criminal Code and the Code on Administrative Offences.

[1] All translations from Russian into English are the author's. The author thanks Professor Nicholas Tsagourias and Dr Russell Buchan for their valuable comments on an earlier draft of this chapter. All websites were last accessed on 11 July 2021.

[2] See 'Russian cyber-attack spree shows what unrestrained internet warfare looks like', *The Guardian* (20 October 2020) https://www.theguardian.com/technology/2020/oct/19/russian-hackers-cyber-attack-spree-tactics.

[3] See Andrew E. Kramer, 'Russia, This Time the Victim of a Cyberattack, Voices Outrage', *New York Times* (14 May 2017) https://www.nytimes.com/2017/05/14/world/europe/russia-cyberattack-wannacry-ransomware.html.

2.1 Constitutional Provisions

The Constitution of the Russian Federation was adopted on 12 December 1993 and came into force on 25 December 1993.[4] It has been amended on a few occasions, most substantially in 2020.[5] The Constitution contains a few provisions having direct or indirect bearing upon cyberspace. For this chapter's purpose, the key notions of constitutional law are sovereignty and jurisdiction. Article 4(1) stipulates that '[t]he sovereignty of the Russian Federation extends to its entire territory', and Article 4(2) states that '[t]he Constitution of the Russian Federation and federal laws shall have supremacy throughout the territory of the Russian Federation'. According to a major Soviet monograph on sovereignty, 'sovereignty [was] the most important, cardinal notion of the State and international law'.[6] A leading post-Soviet Russian treatise on the theory of State and law explains that:

> [a]t present, the recognition of the State as sovereign is important in several respects. Firstly, because only a sovereign State can be an equal participant in the international community, and, secondly, because only a sovereign State can independently create its own supreme central bodies of State power and have powers sufficient to determine the foundations of [the country's] domestic and foreign policy.[7]

Importantly, the same treatise notes that '[s]overeignty [is] unlimited, although not absolute',[8] and infers from sovereignty a State's ability to assert legislative, executive and judicial jurisdiction within its own borders.[9] In line with this understanding, the Federal Laws referred to in section 2.2 below apply throughout the territory of the Russian Federation and, with due regard to applicable rules of international law, may also apply extraterritorially. Rules on extraterritorial jurisdiction are especially relevant in the context of criminal and administrative law (see *infra* sections 6 and 7).

With the enactment of the most recent amendments to the Constitution, the relationship between Russia's domestic law and international law is likely to become more complex. In accordance with Article 15 of the Constitution (which remained unchanged), 'the generally recognized principles and norms of international law and international treaties of the Russian Federation are an integral part of its legal system. If an international treaty of the Russian Federation establishes rules other than those provided by law, then the rules of the international treaty are applied'. However, the amended edition of Article 79 now reads:

---

[4] For the text of the Constitution (in Russian) see: http://www.consultant.ru/document/cons_doc_LAW_28399/.

[5] See Yulia Ioffe, 'The Amendments to the Russian Constitution: Putin's Attempt to Reinforce Russia's Isolationist Views on International Law?' (20 January 2020) EJIL: *Talk!*, https://www.ejiltalk.org/the-amendments-to-the-russian-constitution-putins-attempt-to-reinforce-russias-isolationist-views-on-international-law/.

[6] See Igor D Levin, *Suverenitet* [Sovereignty] (Yuriduchesky Center Press 2003) 11. The original monograph was published in 1948.

[7] See MN Marchenko, *Obshchaya teoriya gosudarstva i prava, tom 1* [General Theory of State and Law, volume 1], 2nd edition (Moscow, Zertsalo-M, 2002) 140.

[8] Ibid., 109.

[9] Ibid., 111.

> The Russian Federation may participate in interstate associations and delegate to them part of its powers in accordance with the international treaties of the Russian Federation, if this does not entail restrictions on the rights and freedoms of man and citizen and does not contradict the foundations of the constitutional system of the Russian Federation. *Decisions of interstate bodies adopted on the basis of the provisions of international treaties of the Russian Federation in their interpretation contrary to the Constitution of the Russian Federation, are not subject to execution in the Russian Federation* (emphasis added).

From the perspective of Russia's domestic law, the second sentence of Article 79 effectively reinforces the primacy of Russia's Constitution over international law. It remains to be seen in the near future how the Russian Constitutional Court will apply this amended provision, given that quite a few cases are pending against the Russian Federation at various international courts,[10] and the provision must have been amended to render the enforcement of their decisions impossible on the territory of the Russian Federation. One may presume, however, that the Constitutional Court's practice of rejecting decisions of international courts and other inter-State bodies based on the second sentence of Article 79 might lead to further complications for Russia under the law of State responsibility.[11]

Constitutional provisions dealing with human rights and fundamental freedoms apply both offline and in cyberspace. Article 17(1) stipulates that 'human and civil rights and freedoms are guaranteed in accordance with universally recognized principles and norms of international law and in accordance with this Constitution'. Article 18 specifies further that '[h]uman and civil rights and freedoms are directly applicable'. Under Article 23(1), '[e]veryone has the right to inviolability of private life, personal and family secrets, protection of his honour and good name', and the second paragraph of the same Article stipulates that '[e]veryone has the right to privacy of correspondence, telephone conversations, postal, telegraph and other messages. Restriction of this right is allowed only on the basis of a court decision'. Further, under Article 24(1), '[c]ollection, storage, use and dissemination of information about the private life of a person without his consent is not allowed'. Article 29(4) provides that '[e]veryone has the right to freely seek, receive, transmit, produce and distribute information in any legal way', and Article 29(5) qualifies that '[f]reedom of the media is guaranteed', and '[c]ensorship is prohibited'. Article 43(5) explains that the Russian Federation 'supports various forms of education and self-education' and this gained a new practical significance in the context of the COVID-19 pandemic. Likewise, the temporary transition of judicial activity to an online format gave new meaning to Article 46(1) (which provides that '[e]veryone is guaranteed judicial protection of his rights and freedoms') and Articles 47–54 (which deal with the right to a fair trial).

According to Kittichaisaree, the most notable human rights pertaining specifically to cyberspace include the right to privacy, freedom of expression as well as anonymity and the right to be forgotten.[12] In the Russian context, circumstances of one's private life and personal data are protected as confidential information, under applicable civil and criminal law (see

---

[10] See Kateryna Busol, 'Can Ukraine's Appeal to the International Courts Work?', https://www.chathamhouse.org/2020/04/can-ukraines-appeal-international-courts-work.

[11] *Cf* art 10 of the Draft articles on Responsibility of States for Internationally Wrongful Acts 2001: 'The responsible State may not rely on the provisions of its internal law as justification for failure to comply with its obligations under this Part'.

[12] See Kriangsak Kittichaisaree, *Public International Law of Cyberspace* (Springer 2017) 45–94.

infra section 5.1). Freedom of expression in cyberspace is subject to some lawful restrictions under the Code of Administrative Offences (see *infra* section 6). In turn, and as noted by Kittichaisaree, Russia's legislation on the right to be forgotten may not be compatible with relevant laws elsewhere:

> [U]sers of search engines in Russia will see full search results pertaining to European users notwithstanding the latter's requests to the search engine providers to have links to their personal information removed [...] In other words, while users of Google and other search engines in EU-Member states will find search results which are edited to comply with requests for the right to be forgotten, users in Russia will see the search results in the original version before any change thereto is made anywhere outside Russia to comply with the right to be forgotten.[13]

As far as information about users within Russia is concerned, they have the right to request search engine operators to remove information:

> which is unreliable, as well as irrelevant, has lost its meaning for the applicant due to subsequent events or actions of the applicant, with the exception of information about events containing signs of criminally punishable acts, the terms of bringing to criminal responsibility for which have not expired, and information about the commission of a crime by a citizen for which conviction has not been removed or canceled

(cf. Article 10.3 of the Federal Law 'On Information, Information Technologies and on the Protection of Information', cf. *infra* section 2.2.4). It has been observed that '[...] telecom operators, as a rule, reject [citizens' applications] lawfully and fairly, the reason being the mistakes [on the part of] applicants themselves in the interpretation and application of the right to be forgotten'.[14]

2.2 Legislation Relative to Cyberspace

The Russian Federation has enacted a few pieces of domestic legislation specifically dealing with cyberspace. This section provides a chronological overview of four relevant Federal Laws and four Decrees issued by the President (enacting, respectively, two Doctrines and two Strategies). Notably, most of these normative documents do not generally refer to international law and focus, instead, on Russia's national interests and security concerns. Interestingly enough, only one among these documents contains a definition, which comes close to that of 'cyberspace' as such (see infra section 2.2.6).

2.2.1 Federal Law 'On Participation in the International Information Exchange'

The Federal Law No. 85-FZ 'On Participation in the International Information Exchange' was adopted on 5 June 1996 and amended in 2003 and 2004.[15] The Federal Law consists of 23 Articles grouped in four chapters. In accordance with Article 1(1), the purposes of the Federal Law include 'creating conditions for the effective participation of Russia in international

---

[13] Ibid., 93–4 (footnotes omitted).

[14] See: 'Kak pravilno polzovatsya pravom na zabveniye v Rossii' [How to properly exercise the right to be forgotten in Russia], https://digitalrights.center/blog/rtbf_russia/ (in Russian).

[15] See Federal Law No. 85-FZ, http://www.consultant.ru/document/cons_doc_LAW_10929/ (in Russian).

information exchange within the framework of a single world information space, protecting the interests of the Russian Federation, constituent entities of the Russian Federation and municipalities during international information exchange, protecting the interests, rights and freedoms of individuals and legal entities during international information exchange'. Among other things, the Law's substantive provisions regulate restrictions in the implementation of international information exchange (Art 8); access to means of international information exchange and foreign information products (Art 12); and coordination of activities in the field of international information exchange (Art 15). The fact that this Federal Law has only been amended twice since 1996 probably means that greater practical weight in the regulation of the Internet is accorded to bylaws, such as the Doctrine of Information Security (see *infra* section 2.2.2), and to more recent laws.

2.2.2 Doctrine of Information Security of the Russian Federation

On 9 October 2000, the President of the Russian Federation approved a Doctrine of Information Security of the Russian Federation. On 5 December 2016, a new Doctrine of Information Security was enacted by Decree No. 646.[16] In accordance with para 5, the Doctrine develops relevant provisions of the National Security Strategy of 31 December 2015,[17] and serves as a normative foundation for the State policy concerning information security. It does not define cyberspace as such and focuses on the methods and means of ensuring the country´s information security. Among other things, the Doctrine lists Russia's national interests in the information sphere,[18] dwells on major information threats (Part III), and outlines the main directions of Russia's information policy in the military,[19] economic,[20] as well as the science, technology and education spheres.[21] Part V lays down the organization of information security, in particular, as far as the legislative, executive and judicial functions are concerned.

---

[16] See Decree No. 646 by the President of the Russian Federation, http://kremlin.ru/acts/bank/41460/page/1.

[17] See Decree No. 683 by the President of the Russian Federation, http://www.consultant.ru/document/cons_doc_LAW_191669/61a97f7ab0f2f3757fe034d11011c763bc2e593f/ (in Russian). In accordance with para. 1, the Strategy is:

> a basic strategic planning document that defines the national interests and strategic national priorities of the Russian Federation, goals, objectives and measures in the field of domestic and foreign policy aimed at strengthening the national security of the Russian Federation and ensuring the country's sustainable development in the long term.

Two paragraphs in the Strategy are of direct relevance to cyberspace. Para. 21 reads:

> The growing confrontation in the global information space is exerting an increasing influence on the nature of the international situation, due to the desire of some countries to use information and communication technologies to achieve their geopolitical goals, including by manipulating public consciousness and falsifying history.

In turn, para. 22 focuses on combating transnational organised crime:

> New forms of illegal activity are emerging, in particular with the use of information, communication and high technologies. Threats associated with uncontrolled and illegal migration, human trafficking, drug trafficking and other manifestations of transnational organized crime are escalating.

On 2 July 2021, the 2015 Strategy was replaced by a newer edition containing a dedicated section on information security (see infra section 2.2.7).

[18] See para 8.

[19] Ibid., para 21.

[20] Ibid., para 25.

[21] Ibid., para 27.

Importantly, the third sentence in para 19 states:

> The absence of international legal norms regulating interstate relations in the information space, as well as [of] mechanisms and procedures for their application, which [would] take into account the specifics of information technologies, complicates the formation of a system of international information security aimed at achieving strategic stability and equal strategic partnership.

This formulation appears to reduce the applicable international law to treaty law only, and to disregard relevant customary international law.[22] This approach is quite convenient in practical terms, for the alleged absence of international legal regulation in cyberspace implies a greater freedom of action both for State and non-State actors with relative impunity.

2.2.3 Federal Law 'On Communication'

The Federal Law No. 126-FZ 'On Communication' was adopted on 7 July 2003, and was amended on no fewer than 73 occasions between 2003 and 2020.[23] In accordance with Article 3(1), the Federal Law regulates 'relations associated with the creation and operation of all communication networks and communication facilities, the use of the radio frequency spectrum, the provision of telecommunication and postal services on the territory of the Russian Federation and in the territories under the jurisdiction of the Russian Federation'. Of particular significance for our purpose is Chapter 7.1 of the Federal Law entitled 'Ensuring stable, safe and integral functioning of the information and telecommunication network "Internet" on the territory of the Russian Federation'. The Chapter was introduced in the Federal Law on 1 May 2019, and seeks to reinforce State control over the management of the Internet. For instance, paragraph 1 of Article 56(2) obliges owners of international communication lines to inform the State about 'the purpose of using the communication line, as well as about the means of communication installed on the specified communication line'. The other paragraphs in the same Article lay down more specific reporting obligations. Given the quality of current relations between Russia and Western States, one may expect the State control to further be reinforced in the years to come.

2.2.4 Federal Law 'On Information, Information Technologies and on the Protection of Information'

The Federal Law No. 149-FZ 'On Information, Information Technologies and on the Protection of Information' was adopted on 27 July 2006, and was amended on no fewer than 39 occasions between 2010 and 2020.[24] The titles of some of the most significant amendments, which affected the core of the original Law, are quite self-explanatory:

– the establishment of a unified register of domain names, page pointers of sites on the Internet and network addresses that allow identifying sites on the Internet, containing information, the distribution of which is prohibited in the Russian Federation (Art 15.1);

---

[22] For the application of customary law to cyberspace, see generally Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017).

[23] See Federal Law No. 126-FZ, http://www.consultant.ru/document/cons_doc_LAW_43224/ (in Russian).

[24] See Federal Law No. 149-FZ, http://www.consultant.ru/document/cons_doc_LAW_61798/ (in Russian).

- the procedure for restricting access to information expressed in an indecent form that offends human dignity and public morality, obvious disrespect for society, the State, the official State symbols of the Russian Federation, the Constitution of the Russian Federation or bodies exercising State power in the Russian Federation (Art 15.1-1);
- the procedure for restricting access to information distributed in violation of copyright and (or) related rights (Art 15.2);
- the procedure for restricting access to information disseminated in violation of the law (Art 15.3);
- the procedure for restricting access to the information resource of the organizer of information dissemination on the Internet (Art 15.4);
- the procedure for restricting access to information processed in violation of the legislation of the Russian Federation in the field of personal data (Art 15.5);
- the procedure for restricting access to sites on the Internet, which repeatedly and illegally posted information containing objects of copyright and (or) related rights, or information necessary to obtain them using information and telecommunication networks, including the Internet (Art 15.6);
- the procedure for restricting access to copies of blocked sites (Art 15.6-1);
- extrajudicial measures to terminate the violation of copyright and (or) related rights in information and telecommunication networks, including the Internet, taken at the request of the copyright holder (Art 15.7);
- measures aimed at countering the use on the territory of the Russian Federation of information and telecommunication networks and information resources, through which access to information resources and information and telecommunication networks is provided, access to which is limited on the territory of the Russian Federation (Art 15.8);
- the procedure for restricting access to the information resource of a foreign mass media performing the functions of a foreign agent and (or) the information resource of a Russian legal entity established by such a foreign mass media (Art 15.9).

These amendments should, in the foreseeable future, result in the establishment in Russia of a so-called 'sovereign Runet'.[25] The officially declared aims of this reform − formally effective as of 1 November 2019 but requiring more bylaws to be enacted by around 2021 − consist in the protection of the Russian segment of the Internet against external threats, and in ensuring the uninterrupted functioning of the Internet within Russia, if an attempt is made to disconnect it from the global network.[26] However, in practice, the reform is likely to 'force citizens to resort to encryption more often, block trackers, use anonymisers and other similar technologies. Some sites will create their own versions on the dark web, which will guarantee the user

[25] The word 'Runet' is composed of the root words 'Russia' and 'Internet' and means the Russian segment of the Internet, including the content of websites and the information infrastructure within Russia.

[26] See Radio Liberty, 'Zakon o suverennom Runete. Chto proizoydet s internetom v Rossii posle 1 noyabrya' [The Law on the 'Sovereign Runet'. What Will Happen to the Internet in Russia after 1 November], https://www.svoboda.org/a/30245986.html (in Russian). See also the chapter by Tsagourias (Ch 1 of this Handbook).

anonymity'.[27] Generally, the '[i]mplementation of the law will inevitably lead to a general deterioration in the network performance'.[28]

2.2.5 Federal Law 'On the Safety of the Critical Information Infrastructure (CII) of the Russian Federation'

The Federal Law No. 187-FZ 'On the Safety of the Critical Information Infrastructure (CII) of the Russian Federation' was adopted on 26 July 2017.[29] According to Article 1, the Federal Law 'regulates relations in the field of ensuring the security of the critical information infrastructure of the Russian Federation [...] in order to ensure its stable functioning when computer attacks are carried out against it'. Article 7(2) further lays down five categories of CII objects, respectively, having:

- social significance, expressed in the assessment of the possible damage caused to the life or health of people, the possibility of termination or disruption of the functioning of objects to ensure the vital activity of the population, transport infrastructure, communication networks, as well as the maximum time of lack of access to public services for recipients of such services;
- political significance, expressed in assessing the possible damage to the interests of the Russian Federation in matters of domestic and foreign policy;
- economic significance, expressed in the assessment of the possible infliction of direct and indirect damage to the subjects of the critical information infrastructure and (or) the budgets of the Russian Federation;
- environmental significance, expressed in assessing the level of impact on the environment;
- the importance of the object of critical information infrastructure for ensuring the country's defence, State security and law and order.

On the same day, and on the basis of this Federal Law, crucial amendments were made to the Criminal Code of the Russian Federation (see *infra* section 5.4).

2.2.6 Information Society Development Strategy in the Russian Federation

On 9 May 2017, the President of the Russian Federation approved the Information Society Development Strategy for 2017–2030.[30] It is the first strategic document on the development of the information society in Russia.[31] It also appears to be the first programmatic text in the Russian legislation to define 'information space' as a phenomenon coming closest semantically to 'cyberspace'.[32] Unlike all foregoing documents, the Strategy does make an explicit

---

[27] Ibid.

[28] Ibid. For a comprehensive overview of the 'sovereign Runet' reform, see Alena Epifanova, 'Deciphering Russia's 'Sovereign Internet Law': Tightening Control and Accelerating the Splinternet', https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law.

[29] See Federal Law No. 187-FZ, http://www.consultant.ru/document/cons_doc_LAW_220885/ (in Russian).

[30] See Decree No. 203 by the President of the Russian Federation, http://publication.pravo.gov.ru/Document/View/0001201705100002?index=0&rangeSize=1 (in Russian).

[31] Ibid., para 6.

[32] Para 4 of the Strategy defines 'information space' as 'a totality of information resources created by subjects of the information sphere, means of interaction of such subjects, their information systems and the necessary information infrastructure'; ibid.

mention of relevant international law sources such as the 2000 Okinawa Charter on Global Information Society, or the 2003 Declaration of Principles 'Building the Information Society: a Global Challenge in the New Millennium',[33] yet it also reiterates[34] a key idea of the Doctrine of Information Security[35] to the effect that '[i]nternational legal mechanisms that make it possible to defend the sovereign right of states to regulate the information space, including in the national segment of the Internet, have not been established. Most states are forced "on the go" to adapt their state regulation of information and information technology to new circumstances'. The Strategy 'defines the goals, objectives and measures for the implementation of the domestic and foreign policy of the Russian Federation in the field of application of information and communication technologies, aimed at the development of the information society, the formation of a national digital economy, ensuring national interests and implementing strategic national priorities'.[36] The national interests in question include:[37]

- human development;
- ensuring the security of citizens and the State;
- increasing the role of Russia in the world humanitarian and cultural space;
- development of free, sustainable and safe interaction between citizens and organizations, government bodies of the Russian Federation, local government bodies;
- improving the efficiency of public administration, developing the economy and social sphere;
- formation of the digital economy.

Overall, the Strategy reaffirms the growing role of the State in the regulation of cyberspace, including by replacing foreign software and hardware with locally produced analogues and storing data on servers located in Russia,[38] with an ultimate view to creating 'systems that ensure the possibility of stable, safe and independent functioning of the Russian segment of the Internet'. Given the Strategy´s time frame, this goal should presumably be reached sometime before 2030.

2.2.7 National Security Strategy of the Russian Federation

On 2 July 2021, the President of the Russian Federation enacted a National Security Strategy,[39] which replaced a previous Strategy of 2015, and contains a comprehensive section on information security. The new Strategy postulates that the development of information and communication technologies increases threats to the security of citizens, society, and the State;[40] that such technologies are used to interfere in States' domestic affairs, and disrupt their sovereignty and territorial integrity, which constitutes a threat to international peace and security;[41] that the

---

[33] Ibid., para 5.
[34] Ibid., para 17.
[35] *Cf supra* section 2.2.2.
[36] See (n 29) para 1.
[37] Ibid., para 21.
[38] Cf paras 28–31.
[39] See Decree No. 400 by the President of the Russian Federation, http://publication.pravo.gov.ru/Document/View/0001202107030001?index=0&rangeSize=1 (in Russian).
[40] Para. 48.
[41] Para. 49.

number of computer attacks against Russian information resources is growing,[42] and the armed forces of foreign States are practicing actions to incapacitate the objects of Russia´s critical information infrastructure.[43] The Strategy further alleges that a distorted view of historical facts and events in the Russian Federation and the world is imposed on the Internet users,[44] that anonymity in cyberspace facilitates the commission of various crimes,[45] and that the use in the Russian Federation of foreign information technologies and telecommunication equipment increases the vulnerability of Russian information resources.[46] To respond to these challenges and, in particular, to reinforce the Russian Federation´s sovereignty in the information space,[47] the Strategy puts forward a set of 16 interrelated measures,[48] including:

– increasing the security of information infrastructure;
– effective prevention, detection, and suppression of cybercrimes;
– ensuring constitutional rights and freedoms in the processing of personal data;
– strengthening the information security of the Armed Forces;
– ensuring the priority use of Russian information technologies and equipment in the information infrastructure of the Russian Federation;
– conveying reliable information about the domestic and foreign policies of the Russian Federation to the Russian and international audiences.

Quite noticeably, the information security component is much more prominent in the new National Security Strategy than it was in the previous edition, and the Strategy will certainly influence all subsequent legislative and institutional developments pertaining to cyberspace.

2.3 Criminal Code and the Code on Administrative Offences

The Criminal Code of the Russian Federation was adopted on 13 June 1996, and was amended on no fewer than 262 occasions between 1998 and 2020.[49] Chapter 28 of the Criminal Code ('Crimes in the sphere of computer information') is based on a few Federal Laws and the 2000 Doctrine of Information Security of the Russian Federation (see *supra* section 2.2),[50] and includes four provisions.[51] The Russian doctrine of criminal law defines 'computer crimes' as 'acts committed in the sphere of computer processes and aiming at information security, and involving information and computer means'.[52] Russian criminologists single out two main

---

[42] Para. 50.
[43] Para. 51.
[44] Para. 53.
[45] Para. 54.
[46] Para. 55.
[47] Para. 56.
[48] Para. 57.
[49] See Federal Law No. 63-FZ, http://www.consultant.ru/document/cons_doc_LAW_10699/ (in Russian).
[50] Although the Russian Federation has not signed and ratified the 2001 Budapest Convention on Cybercrime, the Russian penal law is largely compatible with arts 4–10 of the Convention. For the ratification status, see https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=vCJPWm3V.
[51] Arts 272, 273, 274, 274, see *infra* section 5.
[52] See G N Borzenkov and V S Komissarov (eds), *Kurs ugolovnogo prava, tom 4, Osobennaya chast* [A Treatise of Criminal Law, volume 4, Special Part] (Moscow, Zertsalo-M, 2002) 634.

motives in the commission of computer crimes − gainful interest or an intellectual challenge consisting in the desire to demonstrate one's professionalism,[53] and appear to agree that 'most computer crimes are manifestations of professional and organised crime, often having the collective transnational character'.[54] The factors contributing to the proliferation of computer crimes include the availability of highly qualified human resources, unemployment among society's intellectual elite, opportunities for quick enrichment coupled with a high degree of latency, insufficient protection of automated data management systems, computer criminals' superior professionalism, limited experience of investigating and prosecuting computer crimes, and legislative limits for prosecution.[55]

Although the title of Chapter 28 mentions 'information', most Russian criminal law scholars agree that the specific object of the crimes in question is *information security*,[56] which includes two distinct but interrelated aspects: (1) ensuring the confidentiality, integrity and accessibility of computer information,[57] and (2) the maintenance of means used for processing such information.[58] The elements of crimes included in Chapter 28 of the Criminal Code are formulated with due regard to these aspects (see *infra* section 6).

In turn, the Code of the Russian Federation on Administrative Offences was adopted on 20 December 2001, and was amended a few hundred times between 2002 and 2020.[59] Chapter 13 of the Code lists some 40 offences in the areas of communication and information, of which at least 16 relate to cyberspace. For an overview of the relevant administrative offences, see infra section 6.

3. INSTITUTIONAL FOUNDATION OF INFORMATION SECURITY

The institutional foundation of information security in the Russian Federation is laid down in Part V of the 2016 Doctrine of Information Security (see *supra* section 2.2.2). In accordance with para. 32 of the Doctrine, the composition of the information security system is determined by the President of the Russian Federation. The first part of paragraph 33 stipulates further that responsibility for ensuring security in cyberspace is distributed between a range of authorities at the federal and local levels:

> The institutional foundation of the information security system is composed of: the Federation Council of the Federal Assembly of the Russian Federation, the State Duma of the Federal Assembly of the Russian Federation, the Government of the Russian Federation, the Security Council of

---

[53] Ibid., 634–5.
[54] Ibid., 635.
[55] Ibid.
[56] Ibid., 637.
[57] Thereby, confidentiality implies a duty to refrain from conveying certain information to third persons without authorization, integrity means the prohibition to alter information without permission from an authorized person, and accessibility means the receipt of data in a timely and unimpeded fashion. See A I Chuchayev (ed), *Ugolovnoye pravo, Osobennaya chast* [Criminal Law, Special Part) 3rd edn (Moscow, Prospect, 2018) 403.
[58] Ibid.
[59] See Federal Law No. 195-FZ, http://www.consultant.ru/document/cons_doc_LAW_34661/ (in Russian).

> the Russian Federation, federal executive bodies, the Central Bank of the Russian Federation, the Military-Industrial Commission of the Russian Federation, interdepartmental bodies created by the President of the Russian Federation and the Government of the Russian Federation, executive bodies of the constituent entities of the Russian Federation, local self-government bodies, judicial authorities that, in accordance with the legislation of the Russian Federation, take part in solving problems of ensuring information security.

According to the second part of paragraph 33, Russia's information security system also includes a range of non-State entities:

> Participants in the information security system are: owners of critical information infrastructure facilities and organizations operating such facilities, mass media and mass communications, organizations of monetary, currency, banking and other areas of the financial market, communications operators, information system operators, organizations engaged in the creation and operation of information systems and communication networks, for the development, production and operation of information security means, for the provision of services in the field of information security, organizations carrying out educational activities in this area, public associations, other organizations and citizens who, in accordance with the legislation of the Russian Federation, participate in solving information security issues.

Thus, Russia's law enforcement action in cyberspace constitutes a form of public-private partnership,[60] whereby the State outsources some technical functions to private entities but retains the overall leadership in the maintenance of cyber security.[61] Importantly, '[the law enforcement agencies] must retain an exceptional right to investigate cybercrimes and carry out operational-search activities in cyberspace'.[62]

4. USE OF FORCE AND INTERNATIONAL HUMANITARIAN LAW

So far, rules of international law on the use of force and the conduct of hostilities in the context of cyberspace have only superficially been dealt with in the contemporary Russian doctrine of international law. This is probably due to the fact that 'many senior scholars of international law in the Russian Federation [...] lack the knowledge of English and other foreign languages',[63] and since they belong to a 'separate epistemological community' of Russian-speaking scholars of international law, 'tied together by a common language, history, and geographical space in the former USSR',[64] the Russian doctrine of international law is largely isolated from

---

[60] See Federal Law No. 224-FZ 'On public-private partnership, municipal-private partnership in the Russian Federation and amendments to certain legislative acts of the Russian Federation', http://www.consultant.ru/document/cons_doc_LAW_182660/ (in Russian).

[61] See A L Osipenko, 'Ob uchastii organov vnutrennih del v sisteme obespecheniya kiberbezopasnosti Rossiyskoy Federatsii' [On the Participation of the Internal Affairs Bodies in the Cybersecurity System of the Russian Federation], in *Obshchestvo i pravo* [Law and Society], issue 3(65) (2018) 35–43, at 39.

[62] Ibid.

[63] See Sergey Sayapin, 'The Post-Soviet Central Asia and International Law: Teaching, Research and Practice', https://www.afronomicslaw.org/2020/09/15/the-post-soviet-central-asia-and-international-law-practice-research-and-teaching/.

[64] See Lauri Mälksoo, *Russian Approaches to International Law* (OUP 2015) 87.

the world's leading international law schools.[65] The domestic legislation relative to the *jus ad bellum* and *jus in bello* makes just a few explicit references to cyberspace, cyber warfare, etc. (mostly, in the context of self-defence), and therefore effectively makes the offensive use of cyber technologies legally permissible in the context of 'hybrid warfare'.

4.1 Hybrid Warfare

Russia's military specialists appreciated the utility of cyber technologies for military purposes early enough. Already in February 2013, Head of the General Staff of the Armed Forces of the Russian Federation, Army General V. Gerasimov delivered a speech and published an article based on that speech, where he explained the importance of 'widespread use of political, economic, *informational*, humanitarian and other non-military measures implemented with the use of the protest potential of the population'.[66] He stated plainly that '[a]ll this [should be] complemented by military measures of a covert nature, including the implementation of *information warfare measures* and the actions of special operations forces'.[67] He further noted usefully that '[n]ew information technologies have made it possible to significantly reduce the spatial, temporal and informational gap between troops and command and control bodies', and that:

> [a]nother factor influencing the change in the content of modern methods of armed struggle is the use of modern robotic systems for military purposes and research in the field of artificial intelligence. In addition to flying drones today, tomorrow the battlefield will be filled with walking, crawling, jumping, and flying robots. In the near future, it is possible to create fully robotic formations capable of conducting independent combat operations.[68]

Ultimately, according to General Gerasimov, '[i]t is necessary to improve actions in the information space, including the protection of [our] own facilities'.[69] These approaches were tested, rather successfully, during the ensuing armed conflict with Ukraine,[70] and were reflected in the domestic legislation relative to the 'critical information infrastructure' (see sections 2.2.5 and 5.4).[71]

---

[65] This is evident, e.g., from the fact that the Tallinn Manual 1.0 and 2.0 International Groups of Experts and other participants did not include a single expert from the Russian Federation.

[66] See V Gerasimov, 'Tsennost nauki v predvidenii' [The Value of Science is in the Foresight], https://www.vpk-news.ru/articles/14632 (in Russian), emphasis added.

[67] Ibid. emphasis added.

[68] Ibid.

[69] Ibid.

[70] *Cf* Gergely Tóth, 'Legal Challenges in Hybrid Warfare Theory and Practice: Is There a Place for Legal Norms at All?' in Sergey Sayapin and Evhen Tsybulenko (eds), *The Use of Force against Ukraine and International Law: Jus Ad Bellum, Jus In Bello, Jus Post Bellum* (Springer 2018) 173–83.

[71] However, it should be noted that on 2 March 2019, General Gerasimov delivered another speech where he revised some essential points in his 2013 doctrine (the new approach became known as the 'Gerasimov 2.0 Doctrine'). As noted by Felgengauer, now, the content of the military strategy, according to Gerasimov, again 'consists in the preparation for war and its conduct by the Armed Forces'. Furthermore, '[...] we are talking about a large-scale, not a local war, says Gerasimov, since the likely opponents are also preparing to fight in earnest'. See P Felgengauer, 'Dobitsya prevoshodstva nad ostalnym chelovechestvom: Nachalnik rossiyskogo Genshtaba formuliruyet programmu podgotovki k masshtabnoy voyne' [Achieve Superiority over the Rest of Humanity: Chief of the Russian General Staff

4.2 Use of Force

The current Military Doctrine of the Russian Federation was enacted on 25 December 2014.[72] In accordance with para 1, the Military Doctrine 'represents a system of views officially accepted in the state on preparation for armed defence and armed defence of the Russian Federation'. Para 12 of the Doctrine alludes to the language of Article 2(4) of the UN Charter and Article 1 of the 1974 Definition of Aggression, and mentions among the main external military dangers 'the use of information and communication technologies for military-political purposes for the implementation of actions contrary to international law, directed against the *sovereignty, political independence, territorial integrity of states* and posing a threat to international peace, security, global and regional stability' (emphasis added). Importantly, the Doctrine does not state explicitly that the use of cyber technologies amounts to the 'use of force', 'armed attack' or 'aggression' in the technical legal sense of these terms, and appears to equate the notions of 'armed attack' and 'aggression',[73] without explaining the scope of the 'use of force'. There are at least two sensible, and not necessarily mutually exclusive, reasons for such, presumably deliberate, vagueness: (1) the key terms employed in the Doctrine were meant to be understood in their technical legal meanings under international law, and it was therefore unnecessary to additionally define them in the Doctrine; (2) the Doctrine should not too significantly restrain Russia's ability to offer military responses to security threats, including in cyberspace. In practical terms, it may be assumed from para 22 of the Doctrine[74] that the use of information and communication technologies reaching the gravity threshold set in para 12 of the Doctrine against Russia or its allies may indeed be regarded as 'aggression', and hence, Russia is likely to exercise its right of self-defence under Article 51 of the UN Charter to repel such a cyber attack, with due regard to the rules of international law applicable to self-defence.

As far as individual criminal responsibility for cyber attacks is concerned, it appears that Article 353[75] of Russia's Criminal Code penalises 'aggressive war', and does not penalize

---

Formulates a Programme of Preparation for a Large-scale War], 9 March 2019, https://novayagazeta.ru/articles/2019/03/09/79808-dobitsya-prevoshodstva-nad-ostalnym-chelovechestvom (in Russian).

[72] See Decree No. Pr-2976 by the President of the Russian Federation, http://www.consultant.ru/document/cons_doc_LAW_172989/ (in Russian).

[73] The Doctrine states that the Russian Federation considers an armed attack as an act of aggression (para. 24) or aggression (para 25). See also Roscini (Ch 14 of this Handbook) and Focarelli (Ch 15 of this Handbook).

[74] *Cf* para 22 of the Military Doctrine:
> The Russian Federation considers it legitimate to use the Armed Forces, other troops and bodies to repel aggression against it and (or) its allies, maintain (restore) peace by the decision of the UN Security Council, other collective security structures, as well as to ensure the protection of its citizens who are behind outside the Russian Federation, in accordance with the generally recognized principles and norms of international law and international treaties of the Russian Federation.

[75] See art 353 of the Criminal Code of the Russian Federation:
1. Planning, preparing or unleashing an aggressive war are punishable with imprisonment for a term of seven to fifteen years.
2. Waging an aggressive war is punishable by deprivation of liberty for a term of ten to twenty years.

Cf GA Esakov (ed), *Kommentariy k ugolovnomu kodeksu Rossiyskoy Federatsii* [Commentary on the Criminal Code of the Russian Federation], 5th edn (Moscow, Prospect, 2014) 529.

'aggression' in the form of cyber attacks.[76] Such grave cyber attacks are likely to be penalized under Article 274[1] of the Criminal Code (see *infra* section 5.4). The relevant provisions of other post-Soviet criminal laws are worded in similarly limited ways.[77] Notably, the new edition of the Criminal Code of the Republic of Uzbekistan could become the first post-Soviet criminal law to penalise the use of cyber technologies in the context of *jus ad bellum*.[78]

4.3 International Humanitarian Law

As far as international humanitarian law (IHL) is concerned, para 15 of the Military Doctrine states explicitly that the characteristic features of modern armed conflicts include exercising 'impact on the adversary in the entire depth of his territory simultaneously in the global information space, in the airspace, on land and at sea' (emphasis added). To this end, para 46 provides for the 'development of forces and means of information warfare' in the Russian Federation. However, as of this writing, the Russian Federation does not appear to have enacted any domestic legislation specifically implementing rules of IHL applicable in cyberspace,[79] although academic dialogue on the subject is ongoing.

In the past few years, the Regional Delegation of the International Committee of the Red Cross (ICRC) in Moscow carried out a number of activities to raise awareness, mostly among representatives of the academic circles, of the applicability of IHL to cyber operations. The overarching idea of such activities is that 'there should be no legal vacuum in cyberspace'.[80] The ICRC´s position is that IHL applies to cyber operations conducted in armed conflicts, as far as the consequences of such operations are comparable with those of conventional operations.[81] In particular, the principles of distinction, proportionality must be complied with, and precautionary measures must be taken to avoid or reduce the causing of harm to civilian

---

[76] For a distinction between 'aggressive war' and 'aggression' see Yoram Dinstein, *War, Aggression and Self-Defence* (CUP 2017) 142–5.

[77] For an overview of various models of the criminalization of aggression in the post-Soviet space, see Sergey Sayapin, *The Crime of Aggression in International Criminal Law: Historical Development, Comparative Analysis and Present State* (Springer 2014) 203, 205; see also Sergey Sayapin, 'The Compatibility of the Rome Statute's Draft Definition of the Crime of Aggression with National Criminal Justice Systems' (2010) 81 *Revue Internationale de Droit Pénal* 165.

[78] See Sergey Sayapin, 'Crimes against the Peace and Security of Mankind in the Revised Edition of the Criminal Code of the Republic of Uzbekistan' (2020) 45 *Review of Central and East European Law* 36, 44. The proposed wording reads as follows:

> Aggression, that is, the use of military force, a cyber attack, or another hostile act against the statehood, territorial integrity or political independence of the Republic of Uzbekistan, as well as in any other way incompatible with [the Charter of the United Nations] [international law], shall be punished […].

[79] Not even the Manual on Legal Work in the Armed Forces of the Russian Federation (approved by Order of the Defence Minister of the Russian Federation No. 717 of 3 December 2015, amended as of 8 November 2018) makes an explicit mention of cyber operations, although IHL rules regulating such operations may be implicit in Part VIII of the Manual ('Legal support for actions of troops (forces) in armed conflicts'). The text of the Manual is available at: http://www.consultant.ru/document/cons_doc_LAW_198291/ (in Russian).

[80] See ICRC, 'V kiberprostranstve ne dolzhno byt pravovogo vakuuma' [There Should be No Legal Vacuum in Cyberspace], interview with Cordula Droege, 16 August 2011, https://www.icrc.org/ru/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm (in Russian).

[81] Ibid. For the application of IHL to cyber war see Part IV of this Handbook.

persons or objects.[82] On the other hand, experts agree that IHL does not apply to cyber operations taking place, and cyber crimes committed, outside armed conflicts, and such non-military activities are subject to other areas of law, including domestic criminal and administrative law (see *infra* sections 5 and 6).

5. COMPUTER CRIMES

The Russian Federation exercises both territorial and extraterritorial jurisdiction with respect to computer crimes. Territorial jurisdiction derives from Article 11(1) of the Criminal Code.[83] In turn, extraterritorial jurisdiction mostly derives from the protective principle (cf. Art 12(3) of the Criminal Code[84]), since computer crimes are directed against information security in the Russian Federation (see *supra* section 2.3). According to Russia's Ministry of Interior, in 2019, about 294,000 computer crimes were registered.[85] The Minister of Interior stated on 26 February 2020 that '[c]onsidering the scale of the spread of cybercrimes, the variety of schemes and methods of their commission, the absence of a single detection algorithm, it is impossible to achieve a radical improvement'.[86]

5.1 Unlawful Access to Computer Information (Art 272)

Article 272 of Russia's Criminal Code penalises unlawful access to computer information.[87] The crime's immediate object is the confidentiality of information − that is, two conditions

---

[82] See ICRC, 'RF: chto obshchego mezhdu kompyuterom i avtomatom Kalashnikova?' [What Does a Computer Have in Common with a Kalashnikov Machine Gun?], 7 June 2016, https://www.icrc.org/ru/document/rf-chto-obshchego-mezhdu-kompyuterom-i-avtomatom-kalashnikova (in Russian).

[83] See art 11(1) of the Criminal Code of the Russian Federation: 'A person who has committed a crime on the territory of the Russian Federation is subject to criminal liability under this Code'. On jurisdiction in cyberspace see Kohl (Ch 4 of this Handbook).

[84] See art 12(3) of the Criminal Code of the Russian Federation:
Foreign citizens and stateless persons who do not permanently reside in the Russian Federation who have committed a crime outside the Russian Federation are subject to criminal liability under this Code in cases where the crime is directed against the interests of the Russian Federation or a citizen of the Russian Federation or a person permanently residing in the Russian Federation without citizenship, as well as in cases stipulated by an international treaty of the Russian Federation or other international document containing obligations recognized by the Russian Federation in the field of relations regulated by this Code, if foreign citizens and stateless persons not permanently residing in the Russian Federation were not convicted of foreign state and are prosecuted on the territory of the Russian Federation.

[85] See: 'Chislo IT-prestupleniy v Rossii vyroslo s nachala goda na 75.2%' [The number of IT crimes in Russia has grown by 75.2% since the beginning of the year], https://www.icrc.org/ru/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm (in Russian).

[86] Ibid.

[87] See art 272 of the Criminal Code of the Russian Federation:
1. Illegal access to legally protected computer information, if this act entailed the destruction, blocking, modification or copying of computer information, – shall be punishable by a fine in an amount of up to 200 thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of up to eighteen months, or correctional labor for a term of up to one year, or restraint of liberty for a term of up to two years, or compulsory labor for a term of up to two years, or imprisonment for the same period.

should be met in order for the crime to be accomplished: (1) specific types of data must be protected by law, and (2) the lawful holder of such protected data should have taken measures to protect it. In accordance with Decree No. 188 issued by the President of the Russian Federation on 6 March 1997, confidential data includes:

- information about facts, events and circumstances of the private life of a citizen, which makes it possible to identify his personality (personal data), with the exception of information subject to dissemination in the media in cases established by federal laws;
- information constituting the secrecy of investigation and legal proceedings, information about the State protection of judges, officials of law enforcement and regulatory bodies, about the State protection of victims, witnesses and other participants in criminal proceedings;
- official information, access to which is limited by State authorities in accordance with the Civil Code of the Russian Federation and federal laws (official secret);
- information related to professional activities, access to which is limited in accordance with the Constitution of the Russian Federation and federal laws (medical, notarial, attorney's secrets, privacy of correspondence, telephone conversations, postal items, telegraph or other messages, and so on);
- information related to commercial activities, access to which is limited in accordance with the Civil Code of the Russian Federation and federal laws (commercial secret);
- information about the essence of the invention, utility model or industrial design prior to the official publication of information about them;
- information contained in the personal files of convicts, as well as information on the compulsory execution of judicial acts, acts of other bodies and officials, except for information that is publicly available in accordance with the Federal Law of October 2, 2007 N 229-FZ 'On the penitentiary proceedings'.

Article 272 establishes criminal liability for illegal access to classified information *stricto sensu*, and not just for getting hold of a storage medium (e.g. a hard drive) without aware-

---

2. The same act, which caused major damage or was committed out of selfish interest, – shall be punishable by a fine in the amount of one hundred thousand to three hundred thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of one to two years, or correctional labor for a term of one to two years, or restraint of liberty for a term of up to four years, either forced labor for up to four years, or imprisonment for the same period.
3. Acts provided for in the first or second part of this Article, committed by a group of persons by prior conspiracy, or by an organized group, or by a person using his official position, – shall be punishable by a fine in an amount of up to 500 thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of up to three years, with deprivation of the right to hold certain positions or engage in certain activities for a term of up to three years, or restraint of liberty for a term of up to four years, or compulsory labor for up to five years, or imprisonment for the same period.
4. The acts provided for in the first, second or third parts of this Article, if they entailed grave consequences or created a threat of their occurrence, the applicable sentence is deprivation of liberty for a term not exceeding seven years.

   Notes. 1. Computer information means information (messages, data) presented in the form of electrical signals, regardless of the means of their storage, processing and transmission. 2. In the articles of this chapter, major damage shall be recognized as damage the amount of which exceeds one million rubles.

ness of its content. Access to information is understood as an opportunity to obtain and use information, and illegality of access means that a perpetrator had to right to obtain and use information. The crime is accomplished at the onset of any socially dangerous consequence listed in paragraph 1 of Article 272.[88]

5.2 Development, Use and Distribution of Malicious Computer Programmes (Art 273)

Article 1261 of the Civil Code of the Russian Federation defines a computer programme as 'an objectively presented set of data and commands intended for the operation of computers and other computer devices in order to obtain a certain result, including preparatory materials obtained in the course of developing a computer program and the audiovisual displays generated by it'. Consequently, according to A I Chuchayev, a malicious computer programme in the sense of Article 273[89] of the Criminal Code is one which (1) is knowingly capable of destroying, blocking, modifying, copying computer information, or neutralising the protection of the latter; (2) is intended for these purposes; and (3) performs these functions without user authorisation. The crime is accomplished at the moment of creating, distributing or using a malicious computer programme.[90]

---

[88] See Chuchayev (n 57) 405–6.

[89] See art 273 of the Criminal Code of the Russian Federation:

1. Creation, distribution or use of computer programs or other computer information, knowingly intended for unauthorized destruction, blocking, modification, copying of computer information or neutralization of means of protecting computer information, – shall be punishable by restraint of liberty for a term of up to four years, or compulsory labor for a term of up to four years, or imprisonment for the same term, with a fine in the amount of up to 200 thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of up to eighteen months.
2. Acts provided for in the first part of this Article, committed by a group of persons in a preliminary conspiracy, or by an organized group, or by a person using his official position, as well as causing major damage or committed out of selfish interest, – shall be punished with restraint of liberty for a term of up to four years, or compulsory labor for a term of up to five years with or without deprivation of the right to hold certain positions or engage in certain activities for a term of up to three years, or imprisonment for a term of up to five years with a fine in the amount of one hundred thousand to two hundred thousand rubles or in the amount of the wages or other income of the convicted person for a period of two to three years or without it and with the deprivation of the right to hold certain positions or engage in certain activities for a period of up to three years or without it.
3. The acts provided for in the first or second parts of this Article, if they entailed grave consequences or created a threat of their occurrence, the applicable sentence is deprivation of liberty for a term not exceeding seven years.

[90] See Chuchayev (n 57) 406–7.

5.3 Violation of the Rules for the Operation of Storage, Processing or Transmission of Computer Information and Information and Telecommunication Networks (Art 274)

Article 274[91] of the Criminal Code penalises, in particular, untimely maintenance of components and assemblies, incorrect connection of a computer to power supplies, failure to perform backup, refusal to use antivirus software, processing confidential information outside the workplace, etc.[92] The crime is accomplished when major damage is caused. Unlike the other computer crimes discussed above, which can be committed by any person above the age of 16 years, the crime under Article 274 can only be committed by a person whose professional functions include using or servicing a computer.[93]

5.4 Inappropriate Impact on the Critical Information Infrastructure of the Russian Federation (Art 274[1])

Article 274[1] of Russia's Criminal Code was introduced on 26 July 2017.[94] It represents a *lex specialis* with respect to Articles 272–274 in that it reproduces in paras 1–3 the elements of the respective offences in connection with the 'critical information infrastructure of the Russian

---

[91] See art 274 of the Criminal Code of the Russian Federation:

1. Violation of the rules for the operation of means of storage, processing or transmission of protected computer information or information and telecommunication networks and terminal equipment, as well as the rules for access to information and telecommunication networks, resulting in the destruction, blocking, modification or copying of computer information, causing major damage – shall be punishable by a fine in an amount of up to 500 thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of up to eighteen months, or correctional labor for a term of six months to one year, or restraint of liberty for a term of up to two years, or compulsory labor for a term of up to two years, or imprisonment for the same period.
2. The act provided for in the first part of this Article, if it entailed grave consequences or created a threat of their occurrence, - shall be punishable by compulsory labor for a term of up to five years, or imprisonment for the same term.

[92] See Chuchayev (n 57) 408.

[93] Ibid., 409.

[94] See art 274 of the Criminal Code of the Russian Federation:

1. Creation, distribution and (or) use of computer programs or other computer information, knowingly intended to improperly influence the critical information infrastructure of the Russian Federation, including for the destruction, blocking, modification, copying of information contained in it, or neutralization of protection means the specified information, – shall be punishable by compulsory labor for a term of up to five years, with or without restraint of liberty for a term of up to two years, or imprisonment for a term of two to five years, with a fine in the amount of five hundred thousand to one million rubles, or in the amount of the wage or salary, or any other income of the convicted person for period from one to three years.
2. Unlawful access to protected computer information contained in the critical information infrastructure of the Russian Federation, including the use of computer programs or other computer information, which are deliberately intended to unlawfully influence the critical information infrastructure of the Russian Federation, or other malicious computer programs, if entailed causing harm to the critical information infrastructure of the Russian Federation, – shall be punishable by compulsory labor for a term of up to five years, with a fine in the amount of five hundred thousand to one million rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of one to three years, and with or without restraint of liberty for a term of up to two years, or deprivation freedom for a term of two to six years with a fine in the amount of five

Federation' as defined in the 2017 Law (see *supra* section 2.2.5). In practical terms, it means that an offence against an element of the critical information infrastructure must be qualified under Article 274[1] and not under Articles 272−274. Given the gravity of the crime in question, the sanctions provided for in Article 274[1] are relatively stricter than those provided for under the foregoing Articles.

6. ADMINISTRATIVE OFFENCES IN THE AREAS OF COMMUNICATION AND INFORMATION

The Russian Federation's legislation on administrative offences rests predominantly on the principle of territorial jurisdiction, with elements of extraterritorial jurisdiction.[95] Chapter 13 of the Code on Administrative Offences contains at least 16 offences relative to cyberspace. These are fairly self-explanatory and include:

---

hundred thousand to one million rubles or in the amount of the convicted person's wages or other income for a period of one to three years.

3. Violation of the rules for the operation of storage facilities, processing or transmission of protected computer information contained in the critical information infrastructure of the Russian Federation, or information systems, information and telecommunication networks, automated control systems, telecommunication networks related to the critical information infrastructure of the Russian Federation, or access rules to the specified information, information systems, information and telecommunication networks, automated control systems, telecommunication networks, if it caused damage to the critical information infrastructure of the Russian Federation, – shall be punishable by forced labor for a term of up to five years, with or without deprivation of the right to hold certain positions or engage in certain activities for a term of up to three years, or by deprivation of liberty for a term of up to six years, with deprivation of the right to hold certain positions or engage in certain activities for a term of up to three years, or without one.
4. Acts provided for by part one, two or three of this Article, committed by a group of persons in a preliminary conspiracy or by an organized group, or by a person using his official position, – are punished with imprisonment for a term of three to eight years, with or without deprivation of the right to hold certain positions or engage in certain activities for a term of up to three years.
5. Acts provided for by part one, two, three or four of this Article, if they entailed grave consequences, – shall be punishable by imprisonment for a term of five to ten years with or without deprivation of the right to hold certain positions or engage in certain activities for a term of up to five years.

[95] See art 1.8 of the Code of the Russian on Administrative Offences:

1. A person who has committed an administrative offense on the territory of the Russian Federation shall be subject to administrative liability in accordance with this Code or the law of a subject of the Russian Federation on administrative offenses, with the exception of cases provided for by an international treaty of the Russian Federation.
2. A person who has committed an administrative offense outside the Russian Federation is subject to administrative liability in accordance with this Code in the cases provided for by an international treaty of the Russian Federation, as well as in the cases provided for by part 3 of this article.
3. A legal entity that has committed an administrative offense under art 19.28 of this Code [Illegal remuneration on behalf of a legal entity] outside the Russian Federation is subject to administrative liability in accordance with this Code in the event that the said administrative offense is directed against the interests of the Russian Federation, as well as in cases provided for by an international treaty of the Russian Federation, if the specified legal entity has not been brought to criminal or administrative responsibility in a foreign state for the relevant actions.

- the use of communication facilities or non-certified coding (encryption) facilities that have not passed the procedure for confirming their compliance with the established requirements (Art 13.6);
- failure to comply with the established rules and regulations governing the design, construction and operation of communication networks and facilities (Art 13.7);
- violation of the legislation of the Russian Federation in the field of personal data (Art 13.11);
- violation of rules on the protection of information (Art 13.12);
- illegal activity in the field of information protection (Art 13.13);
- disclosure of information with limited access (Art 13.14);
- impeding the confident reception of radio and television programs and the operation of websites on the Internet (Art 13.18);
- violation of the requirements of the legislation on the storage of documents and information contained in information systems (Art 13.25);
- violation of the requirements for the organization of access to information on the activities of State bodies and local self-government bodies and its placement on the Internet (Art 13.27);
- violation of the requirement to locate technical means of information systems on the territory of the Russian Federation (Art 13.27.1);
- failure to comply with statutory requirements by a person acting on behalf of a telecom operator, or failure by a telecom operator to comply with the established procedure for identifying subscribers (Art 13.30);
- failure to fulfil obligations by the organizer of information dissemination on the Internet (Art 13.31);
- violation of obligations stipulated by the legislation of the Russian Federation in the field of electronic signature (Art 13.33);
- failure by a telecom operator providing services to provide access to the information and telecommunications network 'Internet', the obligation to restrict or resume access to information, access to which should be limited or renewed on the basis of information received from the federal executive body exercising control functions and supervision in the field of communications, information technology and mass communications (Art 13.34);
- dissemination of information by the owner of an audiovisual service containing public calls for terrorist activities, materials publicly justifying terrorism, or other materials calling for extremist activities or substantiating or justifying the need for such activities (Art 13.37);
- failure to perform duties by a search engine operator (Art 13.40).

Notably, most administrative offences included in Chapter 13 can be imputed not only to individuals but also to legal entities. In the absence of criminal responsibility of legal entities in the Russian Federation, administrative measures are quite convenient, in practical terms, for exercising control over activities in cyberspace.

7. CONCLUSION

It appears that Russia will continue reinforcing the domestic regulation of cyberspace, while keeping a convenient distance from international legal developments in this area. Not being

bound by rules of 'hard' international law pertaining to cyberspace gives a State a sense of freedom, which one might not want to give up easily. Russia's plans to construct a 'sovereign Runet' and recent legislative developments to the effect of reducing the role of international law in Russia's legal system, suggest that there is a growing isolationist trend, which may dominate Russia's politics and economy over the next few years. Given Russia's influence in the post-Soviet space, it may also be expected that quite a few other post-Soviet States will model their relevant laws and practices on Russia's example.

26. Chinese approaches to cyberspace governance and international law in cyberspace

Zhixiong Huang and Yaohui Ying[1]

1. INTRODUCTION

The year 2019 witnessed the 50th anniversary of the invention of the Internet and the 25th anniversary of China's full-featured access to the global Internet.[2] No doubt, the Internet has significantly transformed the world in general and China in particular. With the largest number of citizens and the widest Internet-covered areas in the world,[3] China has become one of the core stakeholders in cyberspace, and cyberspace is essential to China's economic development, social stability and national security.[4]

As Malcolm Shaw put it, '[i]n the long march of mankind from the cave to the computer a central role has always been played by the idea of law—the idea that order is necessary and chaos inimical to a just and stable existence'.[5] China understands well that without the stability and predictability provided by rule of law in cyberspace, it is virtually impossible for countries to pursue their common interests through international cooperation. As Ma Xinmin, then Deputy Director-General of the Department of Treaty and Law of Chinese Ministry of Foreign Affairs held in the 6th China-U.S. Internet Industry Forum in 2013, '[w]e need a cyberspace with international rule of law…The rule of law is the best approach to Internet governance because it is in parallel with the development of human civilization today which seeks to operate in a rule-based environment'.[6] This mindset allowed China to join hands with other countries to reach consensus on the importance of a rule-of-law approach to cyberspace gov-

[1] This research is supported by the Major Projects of National Social Science Fund of China (Grant No.: 20&ZD204).

[2] The first use of the Internet as a communications platform was a message sent from UCLA to Stanford via the so-called ARPANET on 29 October 1969; Kal Raustiala, 'Governing the Internet' (2016) 110 *American Journal of International Law* 491, 492–3. China's full-function formal access to the Internet was realized on 20 April 1994. Information Office of the State Council of the People's Republic of China, 'White Paper on the Internet in China' (8 June 2010) http://www.chinadaily.com.cn/china/2010-06/08/content_9950198_3.htm accessed 10 May 2020.

[3] As of March 2020, the number of Internet users in China has reached 904 million, and the Internet penetration rate has reached 64.5 per cent. China Internet Network Information Center, 'The 45th China Statistic Report on Internet Development' (April 2020) 19, http://cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/202004/P020200428399188064169.pdf accessed 30 April 2020.

[4] For example, China had 710 million online shoppers as of March 2020, an increase of 100 million compared to the previous year, and the value of China's online retail in 2019 reached 10.63 trillion Yuan (approximately 1.55 trillion USD); ibid., 39–40.

[5] Malcolm N Shaw, *International Law* (CUP 2014) 1.

[6] Ma Xinmin, 'What Kind of Cyberspace we Need?' (2015) 3 *Contemporary International Relations* 102, 103.

ernance,[7] as is expressed in three reports adopted by the UN Group of Governmental Experts (UN GGE) in 2013, 2015 and 2021, respectively.[8]

Yet this international consensus certainly does not mean countries have the same understanding about how the rule of law in cyberspace is to be realized.[9] From the perspective of China, its approach naturally reflects the country's concerns about how cyberspace is to be governed. More specifically, while the Internet has enormously contributed to China's economic development, its potential 'destabilizing' effects on social stability and national security has also been a major concern in China. For example, China's long dispute with Western countries, especially the US, over its practice of Internet censorship to block and filter online information which it considers harmful to social stability and national security, has triggered its fear about foreign interference into its domestic affairs under the disguise of 'Internet freedom'.[10] The 2013 Snowden revelations regarding US' massive surveillance of the Internet and espionage, including monitoring the communications of top Chinese leaders for years,[11] also added to the worry in China that the US might well abused its dominant position and technological advantages to the detriment of other countries.

All these concerns have deeply shaped the Chinese agenda for international cyber governance and international rule-making. Based on the perception that '[t]he existing global governance system of basic Internet resources hardly reflects the desires and interests of the majority of countries', and '[t]he absence of general international rules in cyberspace that effectively govern the behavior of all parties hampers the development of cyberspace',[12] China aspires to shift from a 'norm-taker' to a 'norm-maker', so as to constrain the hegemony of countries like the US.[13] This also at least partly explains China's desire to build the country into a 'cyber power', which requires that 'the improvement of China's international discourse power and rule-making power in cyberspace' be accelerated.[14]

---

[7] In this chapter, 'cyberspace governance' is used interchangeably with 'Internet governance'.

[8] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security ('2013 GGE Report'), UN Doc. A/68/98, (24 June 2013) para 19; Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security ('2015 GGE Report'), UN Doc. A/70/174 (22 July 2015) para 25; Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security ('2021 GGE Report') UN Doc. A/76/135, 14 July 2021, paras 69–70.

[9] For an analysis of the main areas of difference between the Western and Chinese approaches to the rule of law in cyberspace, see Zhixiong Huang and Kubo Mačák, 'Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches' (2017) 16 *Chinese J.I.L.* 271, 278–301.

[10] White Paper (n 2) Part X.

[11] See, e.g., Der Spiegel, 'NSA Spied on Chinese Government and Networking Firm' (22 March 2014) www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html accessed 30 April 2020. On cyber espionage and international law see Buchan and Navarrete (Ch 11 of this Handbook).

[12] Ministry of Foreign Affairs and Cyber Administration of China, 'International Strategy of Cooperation on Cyberspace' (4 March 2017) http://www.chinaembassy.se/eng/zgxw/t1443121.htm accessed 10 May 2020.

[13] See Greg Austin, 'International Legal Norms in Cyberspace: Evolution of China's National Security Motivations' in Anna-Maria Osula and Henry Roigas (eds) *International Cyber Norms: Legal, Policy & Industry Perspectives* (CCDCOE 2016) 200.

[14] Xinhua News, 'The Political Bureau of the CPC Central Committee Held the 36th Collective Study on Implementing the Strategy of Cyber Power' (9 October 2016) http://www.gov.cn/xinwen/2016-10/09/content_5116444.htm accessed 28 April 2020.

With this background in mind, this chapter aims at discussing some of the key aspects of Chinese approaches to cyberspace governance and international law in cyberspace.[15] It will first elaborate on China's philosophy in relation to cyberspace governance (Section 2), and then analyse and clarify China's approach[16] to international law in cyberspace (Section 3). A few final remarks will be presented at the end.

2. THE PHILOSOPHY UNDERPINNING CHINESE APPROACHES TO CYBER GOVERNANCE

China's position on international rules of cyberspace is rooted in the larger context of China's philosophy of cyberspace governance. This section will discuss two cornerstones of the philosophy underpinning Chinese approaches to cyber governance, i.e., the idea of 'a community with a shared future in cyberspace' ('a CSFC'), and the 'multilateral plus multi-party' pluralism cyberspace governance model.

(a) A Community with a Shared Future in Cyberspace

The vision of building a CSFC was first unveiled by Chinese President Xi Jinping in his remarks at the Second World Internet Conference held in December 2015 ('Xi's 2015 Remarks'), in which he called upon the international community to jointly build a CSFC on the basis of his five proposals, i.e. speeding up the building of global Internet infrastructure and promoting inter-connectivity, building an online platform for cultural exchange and mutual learning, promoting innovative development of cyber economy for common prosperity, maintaining cyber security and promoting orderly development, and building an Internet governance system to promote equity and justice.[17] Thereafter, this vision was endorsed by a number of official documents, including the *International Strategy of Cooperation on Cyberspace* released in March 2017 ('2017 *International Strategy*'),[18] and became 'a core notion for guiding China's promotion of international cooperation in and global governance of cyberspace'.[19]

It should be noted that the vision of building a CSFC is an embodiment and major practice of the idea of 'a community with a shared future for mankind' (a 'CSFM'),[20] the flagship idea

---

[15] The term 'international law in cyberspace' used in this chapter includes both hard (treaty and custom) law and soft law.

[16] Unless otherwise indicated, the word 'China' used in this chapter refers to the official position of Chinese government.

[17] 'Full text: Xi Jinping's Remarks at the 2nd World Internet Conference' (16 December 2015) http://www.china.org.cn/chinese/2015-12/31/content_37432076.htm?W=9776242852 accessed 28 April 2020.

[18] The 2017 *International Strategy* quoted President Xi's call to jointly build a CSFC at the very beginning of the document; International Strategy (n 12).

[19] See Wang Qun (Director-General of the Department of Arms Control of Chinese Ministry of Foreign Affairs), 'China's Proposition: Jointly Building a Community with a Shared Future in Cyberspace' (in Chinese) (2 March 2017) http://world.people.com.cn/n1/2017/0302/c1002-29117319.html accessed 18 May 2020.

[20] The Organizing Committee of the World Internet Conference, '*Jointly Building a Community of Shared Future in Cyberspace*' (17 October 2019) http://www.chinadaily.com.cn/a/201910/17/WS5da7d7b3a310cf3e3557106a_1.html accessed 28 April 2020. This concept paper was officially released

for China's current diplomatic thoughts as well as its proposition for global governance.[21] Indeed, the inter-connectivity of cyberspace and the interdependency of States in this global domain makes the vision of a community with a shared future more real in this virtual world of cyberspace than elsewhere, and the unprecedented opportunity as well as the unprecedented risks and security challenges associated with Internet development in China[22] also allows it to better understand the shared nature of countries in cyberspace. Thus, it can be said that China sees cyberspace as a prioritized area for practicing the larger idea of building a CSFM.

The vision of building a CSFC can be understood through the lens of China's traditional philosophy of 'seeking common ground while reserving difference', which means, in the context of cyberspace, the requirement that '[i]nstead of beggaring thy neighbor, countries should stick together like passengers in the same boat'[23] is even more urgent. Thus, the concept paper *Jointly Building a Community of Shared Future in Cyberspace* officially released in 2019 ('2019 Concept Paper') stated that:

> As countries may have common concerns and diverse aspirations in cyberspace, we should, on the basis of mutual respect for core interests, work for the common good and rise to common challenges. We should enable the Internet to better serve all countries and people in the world, and jointly create an even brighter future for humanity.[24]

This vision also closely relates to China's perception of the flaws of the extant order in cyberspace, especially its feeling that '[p]roblems such as unbalanced development, inadequate rules and inequitable order in cyberspace have become more evident'.[25] Based on the premise that '[c]yberspace is the common space of activities for mankind' and '[t]he future of cyberspace should be in the hands of all countries',[26] the vision of a CSFC appeals for a multilateral, democratic and transparent global Internet governance system that should be built through equal participation, joint decision-making and shared benefits of the international community. In more practical terms, this includes the following key elements:

- Countries are entitled to participate in Internet governance on an equal footing.
- It is important to ensure equitable distribution of basic resources of the Internet and joint management of critical information infrastructure such as root servers.

---

during the 2019 World Internet Conference to comprehensively explain the background, fundamental principles, path to realization and governance framework of a CSFC.

[21] The vision of building a CSFM first appeared in the report of the 18th National Congress of the Communist Party of China in 2012, and was included in the preamble of China's constitution with the constitutional amendment in 2018. 'Constitution of the People's Republic of China (2018 Amendment)' 11 March 2018 http://en.pkulaw.cn/display.aspx?cgid=7c7e81f43957c58bbdfb&lib=law accessed 25 April 2020.

[22] See Section 1 of this chapter.

[23] 'Work Together to Build a Community of Shared Future for Mankind, Speech by H.E. Xi Jinping, President of the People's Republic of China, At the United Nations Office at Geneva, Geneva, 18 January 2017' (19 January 2017) http://www.xinhuanet.com/english/2017-01/19/c_135994707.htm accessed 28 April 2020.

[24] *Jointly Building a Community of Shared Future in Cyberspace* (n 20).

[25] International Strategy (n 12).

[26] Ibid.

- Relevant international processes should be open and inclusive with greater representations and voice of developing countries.[27]

Thus, by calling for building a CSFC, China aims at transforming and improving the extant order to better respond to the problems and challenges countries are facing in cyberspace, and to ultimately 'make cyberspace a community where [countries] can jointly advance development, safeguard security, participate in governance, and share the benefits'.[28] Nevertheless, it is important to note that this vision should not be understood as an attempt to fundamentally change the *status quo*. Actually, this can be seen from the fact that the Chinese approaches to cyberspace governance and international law in cyberspace are premised on sovereign equality and other principles enshrined in the UN Charter, as will be discussed later.

(b) 'Multilateral plus Multi-party' Pluralism

In Xi's 2015 Remarks, he also made the following statement, which laid the basis for China's 'multilateral plus multi-party' model for cyberspace governance:

> International cyberspace governance should feature a multilateral approach with multi-party participation. It should be based on consultation among all parties, leveraging the role of various players, including governments, international organizations, Internet companies, technology communities, non-government institutions and individual citizens.[29]

A comparison between this 'multilateral plus multi-party' model and the related 'multi-stakeholder' approach will help to illustrate their differences. While the multi-stakeholder' approach reflects the Internet's historical dependency on private- and non-profit-sector expertise and have become central to debates over Internet governance since 2003,[30] it has also been long criticized, for example, for masking the deep and systematic economic and political agenda embedded into the existing power arrangements,[31] and for primarily serving the interests of countries with strong industry and civil society, especially the US, while leaving other countries in a disadvantageous position.[32]

As a country with a long history of an up-down social model,[33] China firmly believes that without a leading role of the government, both its internal stability and its international partici-

---

[27] Ibid. These elements contrast the kind of decision-making 'with one party calling the shots or only a few parties discussing among themselves' described by President Xi Jinping in 2015; Xi's 2015 Remarks (n 17).

[28] *Jointly Building a Community of Shared Future in Cyberspace* (n 20).

[29] Xi's 2015 Remarks (n 17).

[30] Shawn Powers and Michael Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom* (Illinois 2015) 129, 138.

[31] Ibid., Chapter 5 entitled 'The Myth of Multistakeholder Governance', especially 153–4.

[32] As Kal Raustiala argues:

> The long-standing preferences of the United States—an Internet that is broadly open and generally free of direct government control and censorship, in which private firms have a major say and in which the key actors are disproportionately U.S.-based or at least share these values—are best realized by multistakeholderism, not multilateralism.

Raustiala (n 2) 501.

[33] Xingdong Fang and Huailiang Hu, 'Report on China's Cyberspace Security Development in 2014' in Xujun Tang et al (eds), *Development Report on China's New Media* (Springer 2017) 49.

pation in cyberspace governance will be jeopardized. Thus it opined that the multi-stakeholder approach without strong leadership of governments could be 'fragmented and divided with limited function and authorization', with the overall framework lacking 'design and coordination'.[34] It is also China's fear that the multi-stakeholder approach has been used by the dominant powers to effectively depreciate the role of sovereign States in Internet governance. For example, when the US expressed its opposition to a new treaty for the International Telecommunication Union (ITU) to 'take over' some of the Internet governance functions in 2012, its representative stated that: 'Internet policy should not be determined by Member States, but by citizens, communities, and broader society, and such consultation from the private sector and civil society is paramount. This has not happened here.'[35]

Thus, in an effort to re-balance the role of governments and non-State actors, the 'multilateral plus multi-party' pluralism serves as China's proposition for Internet governance. It can be seen that this approach consists of two components, i.e., multilateral *and* multi-party participation in cyberspace governance. As is elaborated in the 2017 *International Strategy,* international cyberspace governance should first follow a multilateral approach, meaning '[c]ountries, big or small, strong or weak, rich or poor, are all equal members of the international community entitled to equal participation in developing international order and rules in cyberspace through international governance mechanisms and platforms, to ensure that the future development of cyberspace is in the hands of all peoples'.[36] In a way, this is also a reflection of the key elements of a CSFC, especially the element of equal participation as mentioned above in Section 2(a). As 'multilateral participation' is primarily defined as an issue among sovereign States, this also highlights the State-centric model for cyberspace governance advocated by China.

Quite logically, China has attached great importance to the role of the UN as the multilateral platform for international cyber governance, arguing that the UN 'as an important channel, should play a leading role in coordinating positions of various parties and building international consensus'.[37] By contrast, some countries' engagement in 'small circles' or even cyber military alliances to customize the so-called 'rules' for themselves is what China has always opposed.[38]

The other component, 'multi-party participation', more closely defines the role of different parties (including sovereign States) in cyberspace governance: 'All parties, including governments, international organizations, Internet companies, technology communities, non-governmental institutions and individual citizens, should play their respective roles in building an all-dimensional and multi-tiered governance platform.'[39]

---

[34] Ma Xinmin, 'Letter to the Editors: What Kind of Internet Order Do We Need?' (2015) 14 *Chinese Journal of International Law* 399, 400.

[35] Terry Kramer, 'U.S. Intervention at the World Conference on International Telecommunications,' Media Note Office of the Spokesperson (13 December 2012).

[36] International Strategy (n 12) Chapter III, Principle 3.

[37] Ibid.

[38] 'Statement by the Cyber Affairs Coordinator of the Ministry of Foreign Affairs at the 13th Annual Conference of the Internet Governance Forum' (13 December 2018) https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/fywj_674643/t1633949.shtml accessed 28 April 2020.

[39] International Strategy (n 12).

In reality, while it is true that the Chinese government has played a 'critical and leading role' as the 'main actors in State governance and international cooperation',[40] it has also condoned substantial involvement by its private sector and civil society with The Internet Corporation for Assigned Names and Numbers (ICANN) and within the World Summit on the Information Society (WSIS) and Internet Governance Forum (IGF), and this involvement has increased in volume over time.[41]

In short, China's 'multilateral plus multi-party' model differs from the multi-stakeholder approach mainly in two aspects: the equal right of all countries to participate in developing international order and rules in cyberspace, and a recalibrated balance among various parties or stakeholders, with an emphasis on the 'critical and leading role'[42] of governments. Yet, given the increasingly important role of private sector and civil society not only rhetorically, but also in reality, the difference between the two should not be over-exaggerated.

3. CHINESE APPROACHES TO INTERNATIONAL LAW IN CYBERSPACE

While China has not published any comprehensive position paper on its approaches to international law in cyberspace,[43] official documents and submissions released by the Chinese government as well as the speeches by Chinese leaders or representatives[44] have shed important light on the position of China on key aspects regarding international rules in this area. The analysis below will focus on two issues relating to the Chinese approaches, i.e., the 'sources' of the law (subsection (a)) and certain substantive content of the law (subsection (b)).

(a) Identification and Development of International Rules for Cyberspace

Given the novelty of international law in cyberspace, a fundamental issue in any discussion of this field would relate to the 'sources' of the law, i.e., where to find the international rules for cyberspace, and how should they be developed? The Chinese approach features a three-pronged method for the identification and development of international rules for cyber-

---

[40] *Jointly Building a Community of Shared Future in Cyberspace* (n 20).

[41] Tristan Galloway and H E Baogang, 'China and Technical Global Internet Governance: Beijing's Approach to Multi-Stakeholder Governance within ICANN, WSIS and the IGF' (2014) 12 *China: An International Journal* 72, 92.

[42] *Jointly Building a Community of Shared Future in Cyberspace* (n 20).

[43] Compare, e.g., French Ministry of Defense, 'International Law Applied to Cyberspace' (9 September 2019) 6–7 https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf accessed 30 April 2020; The Federal Government of Germany, 'On the Application of International Law in cyberspace' (March 2021) https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf#:~:text=Germany%20is%20firmly%20convinced%20that%20international%20law%20is,its%20conviction%20that%20international%20law%2C%20including%20the%20UN. In addition to France and Germany, there is a growing list of states that have publicly announced their views on the subject (including Australia, Austria, Czech Republic, Estonia, Finland, Iran, Netherlands, United Kingdom, Japan and the United States).

[44] For example, the 2017 International Strategy (n 12), the 2019 OEWG Submission (see n 55 below), Xi's 2015 Remarks (n 17), Ma's 2013 Speech (n 6) and 2014 Speech (n 34).

space, which is the combination of applying existing international law, setting new soft law, and formulating new hard law under UN apparatus. All the three methods are, albeit to various extent, subject to dispute, and hence deserve further discussion.

(i) Applying existing international law to cyberspace

Whether and to what extent pre-Internet international law applies in cyberspace has been a matter of controversy.[45] Currently, the general consensus is such 'existing international law' does apply in cyberspace, as was confirmed by the UN GGE in 2013 and 2015 respectively.[46] China, as a member of the UN GGE in 2013 and 2015, agreed to (and contributed to) international consensus reflected in the two reports adopted by the UN GGE.[47] Despite the vital importance of this consensus, a number of key issues remain unresolved. For example, exactly how should existing international law apply in the borderless, inter-connected cyberspace? Can the application of existing international law provide an adequate regulatory framework for cyberspace? What kinds of existing rules should be prioritized in cyberspace? Due to the constraint of space, we will briefly discuss the Chinese position on the latter two questions.

In relation to the second question, some countries and scholars are of the view that the existing international law framework is adequate for cyberspace. For example, the US holds that the novel nature of cyber operations may necessitate the reinterpretation of some of the applicable rules but, by and large, the pre-Internet rules should suffice for the online era.[48]

China has expressed its doubt about the sufficiency of existing international law in cyberspace. Ma Xinmin held that:

> cyberspace has its special characteristics. A lot of unique problems without ready solutions in the existing legal framework are emerging in cyberspace, and it is necessary to formulate new legal rules to solve them, and to codify and progressively develop special rules, or *lex ferenda* of international law for cyber-space, as a component of the body of *lex specialis* for cyberspace.[49]

The controversy over the sufficiency of existing international law is inherently linked with the issue of whether new international treaties are needed. Thus, China has consistently emphasized the need to make new international treaties, especially in such fields as combatting cybercrime and cyberterrorism. This, together with another reason why China is not fully satisfied with the application of existing international law, i.e., the perception that the extant law was made without meaningful participation of non-Western countries and did not fully reflect the interests of those countries, will be discussed below in subsection (a)(iii).

---

[45] Francois Delerue, *Cyber Operations and International Law* (CUP 2020) 1.

[46] 2013 GGE Report (n 8) para 19; 2015 GGE Report (n 8) para 24.

[47] As Ma Xinmin pointed out, '[c]yberspace is not a legal vacuum of international law', and '[i]n principle, existing international law, including the UN Charter, should apply to cyberspace'; Ma (n 34) 401.

[48] The White House, 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World' (9 May 2011) 9 www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf accessed 30 April 2020. But for a different view, see Duncan Hollis, 'New Tools, New Rules: International Law and Information Operations' (24 August 2007) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1009224 accessed 30 April 2020, arguing that when applied to information operations, existing international law suffers from 'several, near-fatal conditions', including uncertainty, complexity, and insufficiency.

[49] Ma (n 34) 401.

As to the third question, while in previous years the discussion on how international law applies to cyberspace largely centred on the *jus ad bellum*, law of armed conflict (LOAC) and countermeasures, China challenges the utility of applying such rules in cyberspace. Instead, China attaches high importance to the application of general principles of international law enshrined in the UN Charter, such as the principles of sovereign equality, non-use of force, and peaceful settlement of disputes.[50] This difference, in our view, relates to divergent understandings about what rules best serve the interest of cyber stability, and also to the asymmetric power position of countries in cyberspace – States that wield the greatest power generally seek the greatest latitude for their actions and thus usually endorse permissive norms of behaviour. Conversely, as a rule, weaker States support restrictive norms, seen as shields against their more powerful adversaries.[51]

(ii) Developing new soft law

Currently, international rules for cyberspace consist predominantly of soft law norms, and the 11 voluntary, non-binding 'norms, rules or principles of responsible behaviour of States' proposed by the fourth UN GGE in July 2015 are by far the most internationally recognized soft law norms for cyberspace,[52] with similar initiatives popping up at a surprising rate.[53]

China has been supportive of developing soft law for cyberspace. Together with other Shanghai Cooperation Organization Member States, China submitted the non-binding *International Code of Conduct for Information Security* and a revised version to the UN General Assembly in 2011 and 2015 respectively.[54] China's submission to the UN Open-ended Working Group on ICTs (OEWG) in 2019 ('2019 OEWG Submission'), while dealing with six different topics in total, devoted more than half of its length to the topic 'norms, rules and principles of responsible behavior', which shows the importance of this topic for China.[55]

Given China's position that the application of international law in cyberspace is insufficient, the reasons why China supports the development of soft law are relatively straightforward, as such soft law norms allow countries to fill the legal vacuum in areas unregulated (or insufficiently regulated) by existing international law such as transnational data transfer and combatting cyberterrorism. Although the 'voluntary, non-binding' soft law norms also have their drawbacks in ensuring enforcement and providing legal certainty for global cyberspace, this approach is – at least currently – more practical than making new international treaties,

---

[50] See discussion in subsection (b).

[51] Kubo Mačák, 'On the Shelf, but Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law' (2019) 113 *AJIL Unbound* 81, 82–3.

[52] 2015 GGE Report (n 8) para 13.

[53] For example, the Global Commission on the Stability of Cyberspace (GCSC) issued on 12 December 2019 its final report containing eight proposed norms; https://cyberstability.org/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019-1.pdf accessed 7 May 2020.

[54] Letter dated 12 Sept. 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc A/66/359, 14 September 2011; Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc 69/723, 13 January 2015.

[55] 'China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' (12 September 2020) 2 https://www.un.org/disarmament/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf accessed 9 May 2020.

since the voluntary and non-binding nature of such norms provides States with more discretion, making them more easily acceptable for all countries.[56] In the meantime, it seems that China sees international treaties as the preferred method of developing international rules for cyberspace, viewing soft law as a possible byway towards new treaty rules. In its contribution to the OEWG in April 2020, China made the view that '[i]f it comes to a point when all parties reach common and high consensus on these norms, it is totally reasonable to translate them into a more binding international instrument'. In other words, soft law rules could one day become hard law.[57]

While space does not allow us to elaborate, the following six issues specifically addressed in China's 2019 OEWG submission by and large indicate the areas of greatest concern for China in terms of developing new soft law:

(i) States should pledge not to use ICTs and ICT networks to carry out activities which run counter to the task of maintaining international peace and security;
(ii) State sovereignty in cyberspace;
(iii) critical infrastructure protection;
(iv) data security;
(v) supply chain security; and
(vi) counter-terrorism.[58]

(iii) Making new international treaties

While the application of international law in cyberspace and development of soft law are two more accepted 'sources' of international law in cyberspace, the making of new international treaties is far more controversial, and China has played a leading role in promoting this approach. For, example, the 2017 *International Strategy* clearly expressed China's support for 'discussion on an international convention on combating cyber terrorism' as well as 'discussion and formulation within the framework of the UN of a global legal instrument [on cybercrime]'.[59] Using the route that has been taken in developing international law of outer space as 'valuable reference', China also made the proposal to take a three-step approach to set up the international legal regime for cyberspace: first to formulate a general declaration on fundamental principles for activities in cyberspace, second to draft a convention serving

---

[56] For comparative analysis of the respective role of hard and soft law in international governance, see e.g., Kenneth Abbott and Duncan Snidal, 'Hard and Soft Law in International Governance' (2000) 54 *International Organization* 421; Gregory Shaffer and Mark Pollack, 'Hard and Soft Law' in Jeffrey Dunoff and Mark Pollack (eds), *Interdisciplinary Perspectives on International Law and International Relations: The State of the Art* (CUP 2016) 197–218.

[57] 'China's Contribution to the Initial Pre-Draft of OEWG Report' (April 2020) 3 https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf accessed 7 May 2020.

[58] 2019 OEWG Submission (n 55). It's a bit surprising that the issue of 'State sovereignty in cyberspace' was elaborated in the topic 'norms, rules and principles of responsible behavior' rather than 'application of international law'. Actually, by stating that '[i]t is widely endorsed by the international community that the principle of sovereignty applies in cyberspace', the 2019 OEWG Submission itself also acknowledge that cyber sovereignty is based on the application of the (hard law) principle of sovereignty.

[59] International Strategy (n 12).

as a framework charter for cyberspace activities, and third to further enrich, elaborate and develop principles and rules of international law in specific areas or activities of cyberspace.[60]

It should be noted that while China's proposal to make new international treaties has been echoed by many developing countries, most Western countries have consistently rejected calls for new international treaties. For example, in its written comments submitted to the OEWG in April 2020, the US criticized the proposals made by some States for the progressive development of international law, including through the development of a legally binding instrument on the use of ICTs by State that 'lacked specificity and are impractical'; it also took the view that '[w]ithout a clear understanding of States' views on how existing international law applies to ICTs, it is premature to suggest that international law needs to be changed or developed further'.[61]

China's firm support for new international treaties can be explained from two perspectives. On the one hand, China believes that the two methods for developing international rules which are favoured by Western countries – application of existing international law and developing new soft law – are helpful but not fully satisfactory, as discussed above. Thus, there is an objective need for making new treaties. On the other hand, the existing international law was made under the dominance of Western powers, especially the US, and did not fully take into consideration the concerns and interests of developing countries. Hopefully, making new treaties would allow emerging powers like China to have more say in cyberspace. For example, one of the reasons why China supports negotiating a global convention on combatting cybercrime within the framework of the UN is the Budapest Convention on Cybercrime[62] – the only existing comprehensive multilateral treaty specifically dealing with cybercrime[63] – was formulated mainly by Western countries without the participation of and voice from developing countries.[64]

To date, the UN General Assembly has 'decided to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes'.[65] The approval of the resolution by a 79–60 vote with 33

---

[60] Ma (n 34) 400–1.

[61] 'The United States Comments on the Chair's Pre-draft of the Report' (April 2020) https://front.un-arm.org/wp-content/uploads/2020/04/oewg-pre-draft-usg-comments-4-6-2020.pdf accessed 7 May 2020.

[62] For more detailed discussion about the Budapest Convention, see Kastner and Mégret (Ch 12 of this Handbook).

[63] It should be noted that strictly speaking, the cyber-specific Budapest Convention is not part of 'existing international law', but the making of this convention in 2001 could be a good example explaining why pre-Internet international law is not always sufficient and cyber specific international treaties are needed.

[64] Verbatim Record of the Fifty-Sixth Annual Session: Nairobi, 1–5 May 2017, AALCO/56/NAIROBI/2017/VR, p. 142.

[65] Countering the Use of Information and Communications Technologies for Criminal Purposes, Resolution adopted by the General Assembly on 27 December 2019, A/RES/74/247. On May 26 2021, the General Assembly adopted a new resolution entitled 'Countering the use of information and communications technologies for criminal purposes' (A/RES/75/282). In this new resolution, the General Assembly decided upon next steps for the multilateral negotiations to draft the convention.

abstentions[66] well illustrates the political nature of the division: the 79 countries in favour of the resolution are mostly non-Western countries (including China and Russia), while almost all Western countries voted against it.[67] The extent to which the negotiation will fulfil its mandate and provide momentum to future negotiations for new international treaties in other areas remains to be seen.

(b) Substantive Content of International Law in Cyberspace from the Chinese Perspective

Besides the controversies regarding the 'sources' of international law in cyberspace, countries also differ on many of the substantive legal issues in this field. The analysis below will focus on two (hopefully) representative issues: sovereignty (an example of what China supports) and *jus ad bellum*/ LOAC (an example of what China tends to reject).

(i) Sovereignty

Consistent with China's long adherence to the principle of sovereignty in its international relations,[68] the application of the same principle in cyberspace is also the cornerstone of Chinese approaches to international law in cyberspace. Indeed, China is one of the first countries to actively advocate the concept of 'cyber sovereignty'. One early example is the 2010 *White Paper on the Internet in China*, which declared that: 'The Chinese government believes that the Internet is an important infrastructure facility for the nation. Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected.'[69]

In Xi's 2015 Speech, 'respect for cyber sovereignty' was the first of the four principles which in his view must be upheld '[t]o make progress in the transformation of the global Internet governance system'.[70] China has also made great efforts to implement cyber sovereignty domestically,[71] and to propose the concept internationally.[72] China's efforts, among

---

[66] Edith Lederer, 'UN gives green light to draft treaty to combat cybercrime', *Associated Press* (27 December 2019) https://www.sandiegouniontribune.com/news/nation-world/story/2019-12-27/un-gives-green-light-to-draft-treat-to-combat-cybercrime accessed 8 May 2020.

[67] Before the vote, US deputy ambassador Cherith Norman Chalet observed that 'this resolution will undermine international cooperation to combat cyber-crime at a time when enhanced coordination is essential'; ibid.

[68] While that adherence is 'simply misinterpreted in the west as a disregard of the development of international law, or worse still, considered an excuse to evade its international responsibility', according to Ms Hanqin Xue, a prestigious Chinese practitioner in the field of international law and now judge of the International Court of Justice, China's strong upholding of the principle of sovereignty 'rests both upon its historical past as well as its vision of the future world order', and in particular because 'it believes in diversity and mutual respect in international political life'; Hanqin Xue, 'Chinese Observations on International Law' (2007) 6 *Chinese Journal of International Law* 83, 84–5.

[69] White Paper (n 2).

[70] Xi's 2015 Remarks (n 17).

[71] See e.g., Article 25 of the National Security Law of the People's Republic of China (7 July 2015) http://www.npc.gov.cn/npc/xinwen/2015-07/07/content_1941161.htm accessed 12 April 2020; Article 1 of the Cyber Security Law of the People's Republic of China, http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm accessed 12 April 2020.

[72] International Code of Conduct for Information Security (n 54); International Strategy (n 12); 2019 OEWG Submission (n 55) 2.

others, resulted in the confirmation of the application of State sovereignty in cyberspace by the UN GGE in 2013 and 2015 respectively.[73]

In China's 2017 *International Strategy*, the meaning of 'cyber sovereignty' was explained as:

> Countries should respect each other's right to choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs, or engage in, condone or support cyber activities that undermine other countries' national security.[74]

Overall, China attaches huge importance to cyber sovereignty to highlight the role of States in cyberspace governance, and to consolidate the multilateral model. Thus, China's interpretation of cyber sovereignty covers two key aspects:

Internally, the right of countries to 'choose their own path of cyber development, model of cyber regulation and Internet public policies'. This is no doubt China's top priority in relation to cyber sovereignty, which not only coincides with developing countries' reliance on international law based on the principle of sovereignty as 'the last resort … to defend their political system, economic policy or social stability',[75] but also mirrors China's fear about foreign interference into its domestic affairs under the disguise of 'Internet freedom',[76] particularly after its conflict with the US over Google's withdrawal from China in 2010.[77]

Thus, by the Chinese understanding, cyber sovereignty above all denotes the right of a country to independently decide issues within its *domaine réservé*, and the corresponding obligation of other countries not to intervene into its domestic affairs in the cyber realm. In other words, cyber sovereignty is intrinsically linked to the principle of non-intervention.

Externally, the right of countries to 'participate in international cyberspace governance on an equal footing', including the right to jointly formulate international rules. The emphasis laid by China on this aspect of cyber sovereignty not only echoes its efforts to constraint foreign hegemony and safeguard its legitimate interest in cyberspace, *inter alia*, by advocating a CSFC and the 'multilateral plus multi-party' model for cyberspace governance,[78] it also serves as the principal legal justification for those efforts, since the legal equality derived from the principle of sovereignty implies that 'no member of the international community can be placed at a disadvantage: all must be on the same footing.'[79]

Aimed at providing a useful reference to the key parameters of cyber sovereignty in the Chinese context, including the internal and external aspects mentioned above, a paper entitled *Sovereignty in Cyberspace: Theory and Practice* was released during the 2019 World Internet

---

[73] 2013 GGE Report (n 8) para 20; 2015 GGE Report (n 8) para 27.

[74] International Strategy (n 12) Chapter III, Principle 2.

[75] Xue (n 68) 85.

[76] See Section 1 of this chapter.

[77] Google decided to withdraw from China in early 2010 due to its dissatisfaction with China's Internet regulatory measures, and around that time China was faced with accusation by the US (and to a lesser extent other Western countries) that such policies constitute a threat to Internet freedom; Google, 'A New Approach to China' (12 January 2010) www.google.com/press/new-approach-to-china accessed 30 June 2020.

[78] See subsection 2 (a) and (b) of this chapter.

[79] Antonio Cassese, *International Law* (OUP 2005) 52.

Conference.[80] For example, the paper discussed the right a sovereign State has to exercise legislative, administrative and judicial jurisdiction over 'Internet infrastructure, entities, behavior, and information in its territory'.[81] It also addressed the right to self-defence, stating that '[a] sovereign state has the right to take legal and proper measures under the framework of the UN Charter to protect its legitimate rights and interests in cyberspace from external infringement'.[82]

Since 2017, there has been an ongoing debate on whether the principle of sovereignty can be directly applied in cyberspace as a rule containing concrete obligations that can be violated by another State.[83] While China has not made its position crystal clear, there are reasons to infer that it tends to see foreign surveillance of the Internet and espionage involving China as violation of its sovereignty. For example, in the context of the Snowden revelations in 2013, President Xi Jinping stressed in a speech delivered at the National Congress of Brazil in 2014 that '[n]o matter how developed a country's Internet technology is, it just cannot violate the information sovereignty of other countries'.[84]

In recent years, a number of other countries have also spoken out on the application of sovereignty in cyberspace.[85] While it is true that even in the Western world countries still take divergent views regarding the nature and scope of sovereignty in cyberspace, by comparison the most controversial aspect of the Chinese approach is China's resort to cyber sovereignty as a justification for its Internet censorship when faced with accusation by Western countries

---

[80] This paper was jointly released by three Chinese think tanks to elaborate on the concept and fundamental principles of sovereignty in cyberspace, as well as related practices of different countries in recent years. Wuhan University, China Institute of Contemporary International Relations and Shanghai Academy of Social Sciences, 'Sovereignty in Cyberspace: Theory and Practice' (21 October 2019) http://www.wicwuzhen.cn/web19/release/201910/t20191021_11229796.shtml accessed 30 June 2020. Version 2.0 and Version 3.0 of this paper were also released at the World Internet Conference in 2020 and 2021 respectively. Sovereignty in Cyberspace: Theory and Practice (Version 2.0) is available at http://www.cac.gov.cn/2020-11/25/c_1607869925296336.htm; Sovereignty in Cyberspace: Theory and Practice (Version 3.0) is available at http://www.wicwuzhen.cn/web21/information/Release/202109/t20210928_23157328_2.shtml.

[81] Ibid. Yet, it is still difficult to conclude that 'Internet infrastructure, entities, behavior, and information in its territory' define the scope of cyber sovereignty by the Chinese understanding. For example, China's draft Data Security Law submitted for its first reading by the Standing Committee of the National People's Congress, China's top legislature, on 28 June 2020 notably provides that one of the purposes of the law is to 'safeguard national sovereignty, security and development interests', indicating that data may well fall within the scope of cyber sovereignty. The Chinese version of the draft law was published online for comments by the public. National People's Congress, 'Full Text of the Data Security Law (Draft)' (3 July 2020) http://www.npc.gov.cn/flcaw/userIndex.html?lid=ff80808172b5fee801731385d3e429dd&from=groupmessage accessed 4 July 2020.

[82] Sovereignty in Cyberspace: Theory and Practice (n 80). Interestingly, as is mentioned in subsection 3(a)(ii), so far the Chinese government has been unwilling to confirm the application of the right to self-defence in cyberspace, and the Chinese version of this paper also avoided using the expression 'right to self-defense'.

[83] See Michael N Schmitt and Liis Vihul, 'Respect for Sovereignty in Cyberspace' (2017) 95 *Tex L Rev.* 1639; Gary Corn and Robert Taylor, 'Sovereignty in the Age of Cyber' (2017) 111 *AJIL Unbound* 207.

[84] Xi Jinping, 'Carry Forward Traditional Friendship and Jointly Open up New Chapter of Cooperation' (1 September 2014) http://gb.cri.cn/other/chinanews/eng140901.pdf accessed 2 May 2020.

[85] See e.g., French Ministry of Defense (n 43) 6–7.

that such policies constitute a threat to Internet freedom.[86] Considering China's deep concern about its social stability and national security, there is no reason to expect that its adherence to cyber sovereignty will change. Meanwhile, China has also been at pains to balance 'safeguarding sovereignty and security' with 'protecting legitimate rights and interests of citizens'.[87] Gradual reformation and improvement of its Internet censorship policy and legislation, in our view, could be a constructive step towards fulfilling its pledge to '[support] a free and open Internet'[88] and enhancing mutual trust with other countries.

(ii) *Jus ad bellum* and LOAC in cyberspace

In the past two decades, discussion of 'cyber warfare' and *jus ad bellum*/LOAC[89] as the applicable international law has generated great interest, especially in the Western world.[90] China appeared to be rather cautious about this approach:

> From the perspective of maintaining peace and preventing conflict, states should focus on the implementation of such principles as settlement of disputes by peaceful means and refraining from the use or threat of use of force. Willful use of force, punitive and confrontative countermeasures should be prevented … the applicability of the law of armed conflicts and *jus ad bellum* needs to be handled with prudence.[91]

China's 'prudence' on the application of *jus ad bellum* and LOAC in cyberspace can be explained from at least two aspects. Firstly, China attaches great importance to the peaceful use of cyberspace, and renders that too much discussion of the right to resort to force (especially in the name of self-defence) and the application of LOAC would have potential negative impact on international peace and security, aggravating an arms race and militarizing cyberspace.[92] For instance, China has expressed concern that 'this military paradigm disregards the non-use of principle', and that it will affect strategic trust between countries and increase the risk of inter-State misperception and conflict.[93]

Also, given China's relatively weak military cyber capabilities compared to those of major Western powers, in particular the US, and the already decreased strategic trust, it has reasons to worry that China could well be the potential target and victim of use of force in cyberspace.

---

[86] Huang and Mačák (n 9) 293. For example, Brian J Egan, then Legal Adviser of the US Department of State, stated in 2016 that '[s]ome States invoke the concept of State sovereignty as a justification for excessive regulation of online content, including censorship and access restrictions… And sometimes, States also deploy the concept of State sovereignty in an attempt to shield themselves from outside criticism'; Brian Egan, 'International Law and Stability in Cyberspace' (2017) 35 *Berkeley J Int'l L* 169, 175.

[87] International Strategy (n 12) Chapter III.

[88] Ibid.

[89] In this chapter, the law of armed conflicts is used synonymous with international humanitarian law or *jus in bello*.

[90] For example, the *Tallinn Manual on International Law Applicable to Cyber Warfare* prepared by a group of experts from Western countries focused almost exclusively on the application of *jus ad bellum* and LOAC in cyberspace; Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013).

[91] 2019 OEWG Submissions (n 55) 6.

[92] Verbatim Record of the Fifty Fourth Annual Session: Beijing, 13–17 April 2015, AALCO/54/BEIJING/2015/VR, 177.

[93] Verbatim Record of the Fifty Fifth Annual Session: New Delhi (Headquarters) 17–20 May 2016, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, 159.

Thus, it repeatedly made the call that: 'The lawfulness of cyber war should not be recognized under any circumstance. States should not turn cyberspace into a new battlefield.'[94]

As a result of such disagreements, the GGE report in 2015 made no explicit mention of either the right to self-defence or LOAC.[95] The UN GGE's fifth session in June 2017 concluded without releasing a consensus report, largely due to the fundamental disagreements emerged between the GGE's 25 members on the application of *jus in bello* and LOAC in cyberspace.[96] It should be admitted that most States now recognize, albeit to different degrees, that it is unhelpful to rely on the military paradigm as the first port of call when analysing inter-State malicious cyber operations.[97] Yet the complexity of the disagreement on the application of *jus ad bellum* and LOAC lies in the fact that the debate has been very much politicized – from a purely legal point of view, one may well argue that there is no real legal obstacle to the their application. In the latest UN GEE report, countries finally reached preliminary agreement on the application of LOAC in cyberspace. The GGE recognised the need for further study on how and when the principles of LOAC apply to the use of ICTs by States and underscored that recalling these principles by no means legitimizes or encourages conflict.[98] This is good news and reflects the flexibility of China's attitude towards the LOAC in cyberspace. Further clarification of these two important but controversial issues is yet to be addressed by the States.

4. FINAL WORDS

As a firm supporter of the rule of law in cyberspace, China has expressed its belief that a rule-based system for cyberspace governance is indispensable for both China and the rest of the world, and has set '[enhancing] international rule of law in cyberspace' as one of the strategic goals of China's participation in international cyberspace cooperation.[99] China has also pushed for transformation of the global Internet governance system based on its perception of the shared interest of the international community as well as China's own concerns and appeals, with the goal of building in a CSFC. This provides the context to understand the Chinese approaches to cyberspace governance and international law in cyberspace.

Amidst its endeavours to shift from a 'norm-taker' to a 'norm maker', China has formed its own position on the relevant issues concerning international law in cyberspace, ranging from the 'sources' to the substantive content of the law, and has gained growing influence in the international debate in this field. Yet, to become a successful norm entrepreneur, China

---

[94] 2019 OEWG Submissions (n 55) 6.

[95] As a compromise, the report carefully referred to both 'the aspirations of the international community to the peaceful use of ICTs for the common good of mankind', and 'the inherent right of States to take measures consistent with international law and as recognized in the Charter' and 'the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction', which could be interpreted as meaning the right to self-defense and the key principles of LOAC. 2015 GGE Report (n 8) para 28 (c) and (d).

[96] See Michael N Schmitt and Liis Vihul, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms' (30 June 2017) *Just Security*, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ accessed 8 May 2020.

[97] Huang and Mačák (n 9) 303.

[98] 2021 GGE Report (n 8) para 71(f).

[99] International Strategy (n 12) Chapter III.

will have to face up to a number of legal and political challenges. For example, China has put forward some grand ideas and concepts such as a CSFC and 'multilateral plus multi-party' model for cyberspace governance, which have played a vital role in guiding China's participation in international rule-making in cyberspace. When it comes to more concrete legal arguments and application of specific rules, China still has a lot to learn. To illustrate, in the recent discussion about whether the principle of sovereignty can be directly applied as a rule, the voice of China, a country that has attached such great importance to this principle, is simply absent.

As we enter the third decade of the 21st century, international cooperation in cyberspace is now more urgently needed than before. As then UN Secretary-General Ban Ki-moon pointed out in 2015: 'Making cyberspace stable and secure can be achieved only through international cooperation, and the foundation of this cooperation must be international law and the principles of the Charter of the United Nations.'[100]

In the past years, discussion of cyberspace governance and international law in cyberspace suffered from politicization of the debate and lack of trust among the major players, which made international cooperation so difficult. Unfortunately, nowadays we are probably witnessing increasingly fierce geopolitical struggles within and without this global domain. One recent example is the 'surgical' style sanctions the US imposed on Chinese company Huawei in May 2020 to cut off the latter's supply of key computer chips,[101] which has raised concerns about abuse of dominant position by the US to maintain its hegemony, as 'cybersecurity' reasons for the sanctions could merely be an excuse, whereas the key is Huawei's leadership in 5G constitutes a real threat to the technology hegemony of the US.[102] The prospect of a 'cyber cold war' will only further erode mutual trust between the two countries and frustrate further international collaboration. Let us hope this will not become part of a 'new normal', and countries will manage to get back to the normal to facilitate international cooperation on cyberspace governance which is so vital to the security and prosperity of all countries.

---

[100] 2015 GGE Report (n 8) Foreword by the UN Secretary-General.

[101] Kathrin Hille, 'US "surgical" attack on Huawei will reshape tech supply chain' (19 May 2020) https://www.ft.com/content/c614afc5-86f8-42b1-9b6c-90bffbd1be8b accessed 25 May 2020.

[102] Sam Byford, 'Huawei hits back at US as TSMC cuts off chip orders' (18 May 2020) https://www.theverge.com/2020/5/18/21262042/huawei-us-export-tsmc-chip-manufacture accessed 25 May 2020.

27. Cyber security in the Asia-Pacific

Hitoshi Nasu[1]

1. INTRODUCTION

Cyber threats have been characterised as the Asia-Pacific's chief security problem.[2] As Information and Communications Technology (ICT) dependence has continued to permeate Asia-Pacific societies, the significance of securing cyberspace has increasingly been recognised by regional authorities. Over the last decade, the development and implementation of domestic cyber security strategies has been a top priority for many Asia-Pacific nations. National cyber security strategies and policies have been adopted, or updated in response to evolving cyber security threats in a number of countries in the region, such as Australia,[3] Indonesia,[4] Japan,[5] Malaysia,[6] New Zealand,[7] the People's Republic of China (PRC),[8] the Philippines,[9]

[1] The first edition of this chapter was co-authored with Helen Trezise. Although the chapter was substantially revised for the second edition, the author gratefully acknowledges her contribution to the original part of this chapter. The thoughts and opinions expressed in this chapter are those of the author and do not necessarily represent those of the US Government, the US Department of the Army, the US Department of the Navy, the US Military Academy or the US Naval War College.

[2] See, e.g., Robert K Ackerman 'Diverse Pacific Nations share concerns' (2011) 65 *Signal* 59, 62.

[3] Commonwealth of Australia, 'Australia's cyber security strategy' (2016) https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf accessed 31 July 2020; Commonwealth of Australia, 'Cyber security strategy' (2009).

[4] Indonesian Government Badan Siber Dan Sandi Negara, 'Indonesian cyber security strategy' (June 2018) https://bssn.go.id/strategi-keamanan-siber-nasional/ accessed 31 July 2020; Defence Ministry of the Republic of Indonesia, 'Defence white paper' (3rd edn, November 2015).

[5] Japanese Government Ministry of Defence, 'Defence of Japan 2019' (2019) Ch 3–3 https://www.mod.go.jp/e/publ/w_paper/pdf/2019/DOJ2019_Full.pdf accessed 31 July 2020; Japanese Government Information Security Policy Council, 'Cybersecurity strategy' (2018) https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf accessed 31 July 2020.

[6] Malaysian Government Ministry of Science, Technology and Innovation, 'National cyber-security policy' (2006) https://www.nacsa.gov.my/ncsp.php accessed 31 July 2020.

[7] New Zealand Government, 'New Zealand's cyber security strategy 2019' (2 July 2019) https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2019 accessed 31 July 2020.

[8] Cyberspace Administration of China, 'National cybersecurity strategy' (27 December 2016) http://www.cac.gov.cn/2016-12/27/c_1120195926.htm accessed 31 July 2020.

[9] Department of Information and Communications Technology, 'National cybersecurity plan 2022' (May 2017 and revised in July 2019) https://dict.gov.ph/wp-content/uploads/2019/07/NCSP2022-rev01Jul2019.pdf accessed 31 July 2020.

Republic of Korea,[10] Singapore,[11] Thailand,[12] and Vanuatu.[13] The rapidly increasing sophistication, diversity and ingenuity of cyber attacks in the region has meant that such policies must remain dynamic and responsive. The normative environment surrounding the implementation of cyber security policies has also advanced considerably, with the clarification of how international law applies to the conduct of States in cyberspace and where fault lines exist in legal debate.[14]

As the majority of the world's internet users reside in the Asia-Pacific,[15] cyber security in this region is an issue that demands close scrutiny. According to analysis by the Organisation for Economic Co-operation and Development (OECD), most domestic cyber security policies focus on achieving two interconnected objectives: 'strengthening cyber security for the internet economy to further drive economic and social prosperity; and protecting cyber-space reliant societies against cyber-threats'.[16] Therefore, it is in the best interests of States to promote regional cooperation, as the regional dependence on ICT infrastructure grows. With various opportunities emerging in the digital age, countries 'now have a large stake in a … stable and secure internet'.[17] This chapter reviews cyber security policy initiatives by regional institutions in the Asia-Pacific, with a view to considering how regional efforts to develop cyber security norms are hampered by interaction with traditional security challenges that confront many States in the region as these evolve in cyberspace.

---

[10] National Security Office, 'National cybersecurity strategy' (April 2019) https://www.krcert.or.kr/filedownload.do?attach_file_seq=2162&attach_file_id=EpF2162.pdf accessed 31 July 2020.

[11] Cyber Security Agency of Singapore, 'Singapore's Operational Technology Cybersecurity Masterplan 2019' (October 2019) https://www.csa.gov.sg/news/publications/ot-cybersecurity-masterplan accessed 31 July 2020; Cyber Security Agency of Singapore, 'Singapore's cybersecurity strategy' (2016) https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy accessed 31 July 2020.

[12] Office of the National Security Council, 'National cybersecurity strategy 2017-2021' (2017) https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/ThailandNCS.pdf accessed 31 July 2020.

[13] Republic of Vanuatu, 'National cybersecurity policy' (December 2013) https://ogcio.gov.vu/images/Cybersecurity-Policy-EN-FR-BI.pdf accessed 31 July 2020.

[14] See especially Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) [hereinafter Tallinn Manual 2.0]; UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc A/70/174 (22 July 2015); UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc A/68/98 (24 June 2013).

[15] The number of internet users in the Asia-Pacific was reportedly reaching nearly 2.1 billion in 2018: Statista Research Department, 'Number of internet users in selected Asia-Pacific countries 2019' (Statista, 15 November 2019) https://www.statista.com/statistics/265153/number-of-internet-users-in-the-asia-pacific-region/ accessed 31 July 2020.

[16] OECD, 'Cybersecurity policy making at a turning point: Analysing a new generation of national cybersecurity strategies for the internet economy' in *OECD Digital Economy Papers* (No. 211, OECD Publishing 2012) 6.

[17] Australian Government, 'Australia in the Asia Century' (White Paper, October 2012) 238 https://www.defence.gov.au/whitepaper/2013/docs/australia_in_the_asian_century_white_paper.pdf accessed 31 July 2020.

2. GEOPOLITICAL LANDSCAPE AND CYBER SECURITY

Cyber security threats pose a particularly complex challenge for the Asia-Pacific region due to pre-existing geopolitical rivalries, as well as the political, economic, and socio-cultural diversity that characterises this region.[18] Security threats in cyberspace do not arise in a political or socio-economic vacuum, but are often a manifestation or extension of political or socio-economic tensions that already exist in the real world.

First, cyberspace has increasingly been seen as a new domain of battle space in which sovereign States must defend their national interests. For that reason, the notion of cyber security has been elevated to a matter of national security in many States. The 2012 OECD report on the analysis of the cyber security policies of ten OECD countries described 'sovereignty considerations' as an emerging trend in cyber security policy making.[19] This trend is reflected in a number of national cyber security approaches within the Asia-Pacific region, where States commonly describe threats to domestic cyber security as threats to their 'national security'.[20] For example, Australia recognises the multifaceted nature of cyber threats with the potential to compromise its national security,[21] establishing the Information Warfare Division in July 2017 to strengthen the military cyber capabilities and systems.[22] Similarly, Japan views cyber-attacks as 'an asymmetrical means to impede the military activities of adversaries at low cost',[23] while South Korea is preparing for an increasing likelihood of cyber warfare 'where cyber attacks may incur damage equal to that caused by traditional armed attacks'.[24] Indonesia acknowledges cyberspace as the fifth domain of battlefield, where internet-based platforms are used to advance strategic interests of the nation and to support national defence capabilities.[25] For China, cyberspace is an ideological battle space in which the Chinese Communist Party considers the capability to control information and discourse as integral to the security of the regime.[26]

These national security approaches to cyber security are tethered to the pre-existing geopolitical conditions that shape each State's national defence strategies, and even have the potential to escalate geopolitical tensions. The unique characteristics of offensive cyber tools – for example, unlimited geographical coverage of attacks and the difficulty of identifying

---

[18] See generally Robert K Ackerman, 'Cyber security dominates Asia-Pacific agenda' (2011) 65 *Signal* 59 and Nicholas Rees, 'EU and ASEAN: Issues of regional security' (2010) 47 *Intl Politics* 402.

[19] See OECD (n 16) 7.

[20] See generally Michael Portnoy and Seymour Goodman (eds), *Global Initiatives to Secure Cyberspace: An Emerging Landscape* (Springer 2009).

[21] Australian Government Department of Defence, 'Defence White Paper 2016' (2016) para 2.51; Australian Government Department of Defence, 'Defence White Paper 2013' (2013) para 2.82.

[22] Australian Government Department of Defence, 'Information Warfare Division' (undated) https://www.defence.gov.au/jcg/iwd.asp accessed 31 July 2020. New Zealand has followed suit by developing a new cyber support capability to improve the protection of its cyber networks: New Zealand Ministry of Defence, 'Defence White Paper 2016' (June 2016) paras 5.9, 10.14.

[23] 'Defence of Japan 2019' (n 5) 167.

[24] South Korea's national cybersecurity strategy (n 10) 6.

[25] Indonesia's defence white paper (n 4) 9, 15–16, 110.

[26] International Institute for Strategic Studies, *Asia-Pacific Regional Security Assessment 2019* (2019) Ch 5.

the attacker – make them an attractive option to achieve strategic objectives in disguise.[27] As Ackerman notes, '[t]raditional area geopolitical rivalries are enhanced by the potential for cyber operations, and nations once secure behind rugged borders or vast bodies of water now face potential threats to their national infrastructure through a realm that knows no borders'.[28] Indeed, a number of cyber incidents in the region are suspected of being originating from the Democratic People's Republic of Korea (North Korea), with the aim of stealing funds from financial institutions and cryptocurrency exchanges to generate income.[29] Japan's plan to develop defensive cyber capabilities in response to those attacks triggered hostile reaction by North Korea.[30] The tensions between the PRC and the US have also been manifested in cyberspace, in which the People's Liberation Army continues to develop offensive capabilities to deter or degrade an adversary's ability to conduct military operations and intervention.[31] Since the PRC and the US reached an agreement to refrain from cyber espionage in 2015,[32] the targets of disruptive cyber operations have shifted to other parts of the Asia-Pacific, which has led a number of Asia-Pacific countries to develop offensive cyber capabilities.[33]

Second, the political, economic and socio-cultural identity of the Asia-Pacific region is fragmented, as reflected in the disparity of technological capabilities and cyber infrastructure. The rise of globalisation has seen ICT playing a pivotal role in the advancement of national interests as a 'key defining tool…of modern nation-building'.[34] However, as Thomas notes, this 'virtual process' has 'mirrored the uneven pattern of economic development found across East Asia'.[35] As such, there exists a significant digital divide between technologically advanced nations such as Australia, Japan, China, Singapore and South Korea, and less developed countries

---

[27] This raises an issue of attribution under international law. See, e.g., Nicholas Tsagourias, 'Cyber attacks, self-defence and the problem of attribution' (2012) 17 *J of Conflict and Security L* 229.

[28] Ackerman (n 18) 59.

[29] 'Report of the Panel of Experts established pursuant to Resolution 1874 (2009)' (30 August 2019) UN Doc S/2019/691, paras 57–68 and Annex 21.

[30] Julian Ryall, 'North Korea hits out at Japan as cyber arms race heats up', *The Telegraph* (23 May 2019) https://www.telegraph.co.uk/news/2019/05/23/north-korea-hits-japan-cyber-arms-race-heats/ accessed 31 July 2020.

[31] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019* (2019) 56–7. See also Jr Ng, 'China broadens cyber options' *Asian Military Review* (15 January 2020) https://asianmilitaryreview.com/2020/01/china-broadens-cyber-options/ accessed 31 July 2020.

[32] 'Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference' (The White House, 25 September 2015) https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint accessed 31 July 2020.

[33] Edward White et al, 'Asia-Pacific countries fight back after wave of cyber attacks', *Financial Times* (4 October 2018) https://www.ft.com/content/e846aeac-914f-11e8-b639-7680cedcc421 accessed 31 July 2020. See also James A Lewis and Katrina Timlin, 'Cybersecurity and cyberwarfare: Preliminary assessment of national doctrine and organization' (Centre for Strategic and International Studies, 2011) 6, 8–9, 13, 16, 18.

[34] Ubaidillah Masli, 'Cooperation needed on cybersecurity', *The Brunei Times* (Brunei-Muara, 24 May 2013) A01, quoting Colonel (Rtd) Pg Dato Paduka Hj Azmansham Pg Hj Mohamad, speaking at the opening of the 10th ASEAN Regional Forum Security Policy Conference. See also Council of Security Cooperation in the Asia Pacific (CSCAP), 'Ensuring a safer cyber security environment' (Memorandum No. 20, 2012).

[35] Nicholas Thomas, 'Cyber security in East Asia: Governing anarchy' (2009) 5 *Asian Security* 3, 4.

such as Cambodia, Laos, Myanmar, the Philippines, Vietnam, and Timor-Leste.[36] Indonesia has been particularly vulnerable to exploitation of cyberspace for malicious cyber attacks, cybercrimes, and the dissemination of misinformation and disinformation.[37] The result is that some States have been refining cyber security strategies and adapting them to evolving cyber threats for years now, while in other countries, rapidly growing cyber infrastructure and ICT usage have meant that cyber threats are only just becoming, or still yet to become, securitised.

In developing regional cyber security confidence building measures (CBMs), some States are of the view that the particular characteristics of the Asia-Pacific region, including the cyber capacity of less developed countries and domestic differences in political, economic, and socio-cultural orientations, must be duly taken into account.[38] The PRC, for example, considers cyberspace as the nation's new territory for sovereignty,[39] applying tighter government regulation of cyberspace.[40] Australia, on the other hand, has advocated that 'the internet needs to remain open and free of unnecessary government regulation'.[41]

Third, cyber security threats might emanate not just from sovereign States and State-sponsored actors, but also from non-State actors, such as terrorist groups and individuals.[42] Contemporary cyber threats come in a multitude of forms and reflect a range of motivations, from money-making to cyber espionage, sabotage, destabilisation, and other strategic and tactical military advantages. Indeed, concerns have increasingly been raised over the growing threat of cyber intrusion by criminal organisations, as opposed to individual hackers.[43] In addition, the growing volume, complexity, seriousness, and professionalism of such attacks further complicate any efforts to secure and stabilise cyberspace.

The transnational nature of cyber security threats means that unilateral responses and countermeasures alone are unlikely to be effective. This is particularly problematic in a region like the Asia-Pacific where, as Rees explains, 'there are a number of weak States with limited political and institutional capacity to address [cross-border] threats'.[44] Thus, transnational cyber security concerns have increasingly become focal points of key regional bodies, particularly Association of Southeast Asian Nations (ASEAN), its ASEAN-Plus progenies, the ASEAN Regional Forum (ARF), and the Asia-Pacific Economic Cooperation (APEC).[45]

---

[36] See, e.g., Caitríona H Heinl, 'Regional cybersecurity: Moving toward a resilient ASEAN Cybersecurity Regime' (2014) 18 *Asia Policy* 131, 141–3. For example, OceanLotus, a hacking group also known as APT32, operates across Cambodia, Laos, the Philippines and Vietnam: 'OceanLotus adopts public exploit code to abuse Microsoft Office software', *Cyber Security Review* (21 March 2019) https://www.cybersecurity-review.com/news-march-2019/oceanlotus-adopts-public-exploit-code-to-abuse-microsoft-office-software/ accessed 31 July 2020.

[37] Thomas Paterson, 'Indonesian cyberspace expansion: A double-edged sword' (2019) 4 *Journal of Cyber Policy* 216, 219–20.

[38] See, e.g., Kwon Haeryong, 'The ARF perspectives on TCBMs: Future work' (Presented at United Nations Institute for Disarmament Research Cyber Security Conference, Geneva, 8-9 November 2012).

[39] PRC's national cybersecurity strategy (n 8) s 1(1).

[40] Cybersecurity Law 2016 (PRC); Regulations on Internet Security Supervision and Inspection by Public Security Organs 2018 (PRC).

[41] Australia's Asian Century White Paper (n 17) 238.

[42] See Thomas (n 35) 5.

[43] See, e.g., The Philippines national cybersecurity plan 2022 (n 9) 13–5.

[44] Rees (n 18) 408.

[45] Regional leaders consider these institutions to be key players in regional cyber security policy development: 'East Asia Summit Leaders' Statement on Deepening Cooperation in the Security of Information and Communications Technologies and of the Digital Economy' (adopted at the 13th East

Ultimately, the 'digital divide' and the lack of homogeneity amongst Asia-Pacific States, not just economically but also politically and socio-culturally, poses a challenge to the ability of regional forums and institutions to galvanise members into collective action against cyber security threats.[46] However, this disparity can also be considered an advantage within the regional framework, as it means that less developed countries can work within regional institutions to seek assistance and guidance in overcoming inadequacies in ICT capacity and meeting challenges posed by cyber security threats from the outset.[47] As the Council for Security Cooperation in the Asia-Pacific stresses, holistic domestic cyber security policies and regional collective measures of cooperation comprise the two essential conditions required to 'maximise protection against cyber threats and also maximise the regional benefits of the digital economy'.[48] The critical question relevant to this chapter is, therefore, to what extent existing regional institutions in the Asia-Pacific have contributed to attaining these competing goals within their institutional framework.

3. REGIONAL CYBER SECURITY APPROACHES

Over the past decade, Asia-Pacific States have attempted to address an increased variety of non-traditional security issues within regional frameworks.[49] More recently, geopolitical tensions have been rising with actual and possible military confrontations between States involved in territorial and maritime disputes, most notably in the South China Sea. These military and non-military concerns are both influencing the dynamics of the security landscape in the Asia-Pacific. It provides a critical context for understanding the regional engagement with the domain of cyber security over the last two decades and into the future. This section reviews the development of regional cyber security policy initiatives for the purpose of understanding the institutional efforts and obstacles to regional cooperation in securing cyberspace.

(a) Association of Southeast Asian Nations (ASEAN)

ASEAN was founded by Indonesia, Malaysia, the Philippines, Singapore, and Thailand with the aim 'to ensure their stability and security from external interference in any form or manifestation'.[50] From its inception, ASEAN has served its role as a political platform with dual

---

Asia Summit, Singapore, 15 November 2018); '2015 East Asia Summit Statement on Issues Related to Security of and in the Use of Information and Communications Technologies' (Kuala Lumpur, Malaysia, 22 November 2015); 'Chairman's Statement of the 7th East Asia Summit' (Phnom Penh, Cambodia, 20 November 2012). Other regional cyber security initiatives such as the Asia-Pacific Telecommunity (APT) and the United Nations Economic and Social Commission for Asia and the Pacific have a more technical focus on ICT regulation in general. See generally Portnoy and Goodman (n 20) Ch 4.

[46] See Rees (n 18) 408.

[47] See Heinl (n 36) 141, 143; Thomas (n 35) 11.

[48] CSCAP (n 34) 1.

[49] See generally, e.g., Mely Caballero-Anthony and Alistair D B Cook (eds), *Non-Traditional Security in Asia: Issues, Challenges and Framework for Action* (Institute of Southeast Asian Studies, 2013); Mely Caballero-Anthony, Ralf Emmers and Amitav Acharya (eds), *Non-Traditional Security in Asia: Dilemmas in Securitization* (Ashgate 2006).

[50] Declaration Constituting an Agreement Establishing the Association of South-East Asian Nations (8 August 1967, entered into force 8 August 1967) 1331 UNTS 235. ASEAN has expanded its mem-

regional security functions – committing themselves to collective efforts to remove external interference, on the one hand, and entering into reciprocal arrangements to ensure the internal stability and security of the government in each member State, on the other.[51] Both are based on the 1976 *Treaty of Amity and Cooperation in Southeast Asia*:[52] the former is embedded in the regional principle of non-interference in Article 2(c), whereas the member States' commitment to 'endeavour to strengthen their respective resilience in…*security fields*' (emphasis added) in Article 11 supports the latter role. The ASEAN Charter, adopted in 2007, reaffirms these commitments by proclaiming that it aims to 'enhance regional resilience by promoting greater political, security…cooperation' and with 'shared commitment and collective responsibility in enhancing regional peace, security and prosperity'.[53]

ASEAN's cyber security policy has indeed developed along this line of dual functions, although with some modification towards further regional integration and more active engagement with external actors. On the one hand, particularly at the initial stage, ASEAN has attempted to secure cyberspace through regional cooperation in building national cyber security resilience. More recently, ASEAN has realised the need for more comprehensive cyber security efforts in order to secure cyberspace from common threats, such as transnational cyber intrusions by criminal and terrorist organisations.[54]

The initial stage of regional cyber security policy initiatives in ASEAN can be characterised as the cooperative building of national cyber security resilience. Responsibility for ICT infrastructure and capacity development has fallen primarily to the ASEAN Telecommunications and IT Ministers (TELMIN) – now part of the ASEAN Economic Community whose aim is to enhance the region's economic growth and competitiveness.[55] With the aim of bridging the digital divide within the region, TELMIN adopted the *e-ASEAN Initiative* in 1999, and subsequently the *e-ASEAN Framework Agreement* in 2001, looking in part to encourage cooperation between Member States to develop, strengthen and enhance the competitiveness of the regional ICT sector,[56] especially within developing States. The 1998 *Hanoi Plan of Action* also called for the establishment of the 'ASEAN Information Infrastructure', designed to ensure the interconnectivity and interoperability of IT systems within Member States.[57]

In 2003, TELMIN's cyber development goals were combined with cyber security agendas by the *Singapore Declaration*, which called on all ASEAN Member States to establish

---

bership since then, adding Brunei Darussalam, Cambodia, Laos, Myanmar and Vietnam. At the time of writing, the application for membership by Timor-Leste is still being considered.

[51] For details, see especially Amitav Acharya, *Regionalism and Multilateralism: Essays on the Cooperative Security in the Asia-Pacific* (Eastern Universities Press 2003) 227–30.

[52] Treaty of Amity and Cooperation in Southeast Asia (24 February 1976, entered into force 15 July 1976) 1025 UNTS 319.

[53] Charter of the Association of Southeast Asian Nations (20 November 2007, entered into force 15 December 2008) arts 1 and 2(2)(b).

[54] Hitoshi Nasu, Rob McLaughlin, Ronald R Rothwell and See Seng Tan, *The Legal Authority of ASEAN as a Security Institution* (CUP 2019) Ch 5; Thomas (n 35) 11.

[55] See generally 'ASEAN Economic Community Blueprint 2025' (ASEAN Secretariat 2015) para 6 https://www.asean.org/storage/2016/03/AECBP_2025r_FINAL.pdf accessed 31 July 2020; 'ASEAN Economic Community Blueprint' (ASEAN Secretariat 2008) para 6 https://www.asean.org/wp-content/uploads/images/archive/5187-10.pdf accessed 31 July 2020.

[56] See e-ASEAN Framework Agreement (24 November 2001, not in force) art 2.

[57] *Hanoi Plan of Action* (adopted by the 6th ASEAN Summit, Hanoi, Vietnam, 15 December 1998) para 3.1.1.

national Computer Emergency Response Teams (CERTs) by 2005 (following the inauguration of LaoCERT in February 2012, this goal has belatedly been achieved).[58] This formed part of a push by TELMIN to establish a common regional framework for sharing cyber expertise, as well as cyber security threat and vulnerability assessment information, so as to 'help develop cybersecurity policies and exchange real-time information on cybersecurity issues'.[59] Subsequently, in its *Economic Community Blueprint,* ASEAN emphasises the need for a secure and interconnected regional information infrastructure.[60]

Behind this shift in policy focus to a common regional framework is the realisation that promoting regional ICT interconnectivity, and thus interdependence, as a way to strengthen the region's overall stability and prosperity could 'raise the probability of transnational crime and cross-border cyber-related incidents'.[61] Malaysian Minister of Defence Dato' Seri Dr Ahmad Zahid Hamidi made this point clear at the 2012 Asia Security Summit (Shangri-La Dialogue), stating that while ASEAN – and Malaysia in particular – benefitted from regional interconnectivity, 'a major cyber-attack on the network linking its members would have grave implications leading towards destabilisation'.[62] Given that less developed countries are at greater risk of cyber intrusion, this further highlights the need for regional cooperation in capacity building exercises and other cyber security measures aimed at mitigating potential 'weak links'.[63]

The *ASEAN ICT Masterplan 2015* (AIM2015), which was adopted in 2011 to set out ASEAN's quest to become a 'global ICT hub',[64] addresses the potential negative ramifications of increased ICT interconnectivity and interoperability. As Heinl explains:

> The document calls for the development of a common framework for network security, the establishment of minimum standards for network security to ensure the preparedness and integrity of networks, the implementation of a network security 'health screening' program, the development in all sectors of best-practice models for business continuity and disaster recovery, and the establishment of the multi-stakeholder ASEAN Network Security Action Council (ANSAC) to promote CERT cooperation and the sharing of expertise.[65]

ANSAC has met annually since 2012, and its tasks have included reviewing the ASEAN Telecommunication Regulators' Council (ATRC) Framework for Cooperation on Network Security, through which ASEAN TELMIN's work is largely completed.

Thus, in pursuing enhanced regional cyber capacity, interconnectivity and ICT infrastructure within the region, ASEAN leaders started seeing comprehensive cyber security efforts as

---

[58] See ASEAN TELMIN, 'Singapore Declaration' (3rd TELMIN, September 2003); ASEAN TELMIN, 'Joint Media Statement of the Third ASEAN Telecommunications and IT Ministers' (3rd TELMIN, Singapore, 19 September 2003) para 4; Heinl (n 36) 151–2.

[59] ASEAN TELMIN, 'Joint Media Statement of the Third ASEAN Telecommunications and IT Ministers' ibid.

[60] See 'ASEAN Economic Community Blueprint 2025' (n 55) para 51; 'ASEAN Economic Community Blueprint' (n 55) para 51.

[61] Heinl (n 36) 137.

[62] Dato' Seri Dr Ahmad Zahid Hamidi, 'New forms of warfare - Cyber, UAVs and emerging threats' (Speech delivered at the Asia Security Summit, Shangri-La Hotel, Singapore, 3 June 2012).

[63] Heinl (n 36) 137.

[64] 'ASEAN ICT Masterplan 2015' (ASEAN Secretariat 2011) 26 https://asean.org/?static_post=asean-ict-masterplan-2015 accessed 31 July 2020.

[65] Heinl (n 36) 147.

increasingly vital. Cyber security featured in TELMIN's 2012 *Mactan Cebu Declaration*,[66] in which TELMIN made a number of cyber security related undertakings.[67] In 2017, TELMIN endorsed the ASEAN Cybersecurity Cooperation Strategy to guide ASEAN Member States in taking a coordinated approach to building their national cyber security capacity.[68] Moreover, TELMIN acknowledged in its Master Plan for 2025 the challenges of disruptive technologies, urging governments to take initiatives and to establish a policy framework for data sharing, online privacy and cyber security.[69]

ASEAN has also sought to address cyber insecurities along with other regional security issues through its Political-Security Community, whose aim is to establish a 'cohesive, peaceful, stable and resilient region with shared responsibility for comprehensive security'.[70] Within this Community, cyber security has primarily been the domain of the ARF, as will be further examined in the next section. However, through ASEAN Defence Ministers Meetings (ADMMs), it has also been seeking to promote and enhance ASEAN's capacity to address cyber security in the region. In August 2013, at the Second ADMM-Plus meeting held in Brunei Darussalam, ASEAN Defence Ministers and eight ASEAN Dialogue Partners discussed what role the defence sector should play in addressing emerging non-traditional security threats, including cyber security.[71] In May 2016, ASEAN Defence Ministers adopted the Concept Paper on the Establishment of the ADMM-Plus Experts' Working Group on Cyber Security,[72] which focused on cyber security issues related to the defence and military sectors.[73] These activities are designed to enhance cyber security capabilities and develop appropriate mechanisms for cooperation among defence and military sectors.

---

[66] ASEAN TELMIN, 'Mactan Cebu Declaration: Connected ASEAN – Enabling Aspirations' (12th TELMIN, the Philippines, 15-16 November 2012).

[67] Ibid., paras 7–14, 16.

[68] ASEAN TELMIN, 'Joint Media Statement' (17th TELMIN, Siem Reap, Cambodia, 1 December 2017) para 4.

[69] 'Master Plan on ASEAN Connectivity 2025' (ASEAN Secretariat 2017) paras 12–13 https://asean.org/wp-content/uploads/2018/01/47.-December-2017-MPAC2025-2nd-Reprint-.pdf accessed 31 July 2020.

[70] 'ASEAN Political-Security Community Blueprint' (ASEAN Secretariat 2009) para 10 https://asean.org/wp-content/uploads/images/archive/5187-18.pdf accessed 31 July 2020.

[71] ASEAN Secretariat, 'ASEAN Defence Ministers and their Plus Counterparts Reaffirm Commitment for Regional Peace and Security at the 2nd ADMM-Plus' *ASEAN Secretariat News* (3 September 2013) https://asean.org/asean-defence-ministers-and-their-plus-counterparts-reaffirm-commitment-for-regional-peace-and-security-at-the-2nd-admm-plus/ accessed 31 July 2020. The eight ASEAN dialogue partners were Australia, India, Japan, New Zealand, PRC, Russia, South Korea, and the US.

[72] 'Joint Declaration of the ASEAN Defence Ministers on Promoting Defence Cooperation for a Dynamic ASEAN Community' (adopted at the 10th ASEAN Defence Ministers' Meeting, 25 May 2016) para 5.

[73] 'Establishment of the ADMM-Plus Experts' Working Group on Cyber Security: Concept Paper' (adopted at the 10th ASEAN Defence Ministers' Meeting, 25 May 2016) para 6.

(b) ASEAN Regional Forum (ARF)

The ARF was established by ASEAN in 1994 to help promote peace and prosperity across the region,[74] and currently has a membership base of 27 nations.[75] Although it originally emerged as a cooperative platform for confidence building and preventive diplomacy,[76] it has further institutionalised with a common security vision based on the ideas of cooperative security and comprehensive security, as enshrined in the 2009 Vision Statement.[77] It has been designated in *Bali Concord II*, adopted in 2003, as 'the primary forum in enhancing political and security cooperation in the Asia-Pacific region'.[78] As Kurlantzick notes, while the ARF 'has no authority beyond ASEAN's, it provides an opportunity for increased dialogue and interaction' between major regional actors.[79] Cyber security has been addressed within the framework of counterterrorism and transnational crime until the decision was made in 2017 to establish ARF inter-sessional meeting on ICTs security.[80]

Since 2004, the ARF has conducted regular seminars and workshops on cyberspace, with particular focus on cyber terrorism, incident response, capacity building, and the threat of proxy actors. In 2006, the ARF issued the *Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyberspace*,[81] which encouraged Member States to enhance national and regional regimes for cyber security on the grounds that 'an effective fight against cyber-attacks and terrorist misuse of cyber space requires increased, rapid and well-functioning legal and other forms of cooperation'.[82] This policy was endorsed in the *Hanoi Plan of Action to Implement the ARF Vision Statement*, adopted at the ARF senior officials' meeting in May 2010.[83]

ARF cyber security efforts thus follow the 2006 Statement that envisaged cyber security threats posed by non-State actors and transnational crimes as common security challenges

---

[74] See, e.g., 'The ASEAN Regional Forum: A Concept Paper' (adopted by the ASEAN Regional Forum Ministerial Meeting 1 August 1995) para 5 ('1995 Concept Paper').

[75] The 27 members are the ten ASEAN Member States (Brunei, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam), the ten ASEAN dialogue partners (Australia, Canada, China, European Union, India, Japan, New Zealand, Republic of Korea, Russia and the US), and Bangladesh, Democratic People's Republic of Korea, Mongolia, Pakistan, Papua New Guinea, Timor-Leste, and Sri Lanka.

[76] 1995 Concept Paper (n 74) para 6; 'The First ASEAN Regional Forum Ministerial Meeting' (Chairman's Statement, Bangkok, Thailand, 25 July 1994) para 4.

[77] 'ASEAN Regional Forum Vision Statement' (16th ARF, Phuket, Thailand, 23 July 2009).

[78] 'Declaration of ASEAN Concord II' (9th ASEAN Summit, Bali, Indonesia, 7 October 2003) para 6 ('Bali Concord II').

[79] Joshua Kurlantzick, 'ASEAN's Future and Asian Integration' (Council on Foreign Relations, November 2012) 6.

[80] 'Co-Chair's Summary Report: 1st ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of information and Communication Technologies (ARF ISM on ICTs Security)' (Kuala Lumpur, Malaysia, 25–26 April 2018); 'Co-Chair's Summary Report: 15th ASEAN Regional Forum Inter-Sessional Meeting on Counter-Terrorism and Transnational Crime' (Semarang, Indonesia, 6-7 April 2017) para 25.

[81] 'ASEAN Regional Forum Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyberspace' (13th ARF, Kuala Lumpur, Malaysia, 28 July 2006).

[82] Ibid.

[83] 'Hanoi Plan of Action to Implement the ASEAN Regional Forum Vision Statement' (endorsed by ARF SOM on 20 May 2010) para 2.

within the region. Along this line, the 2012 'Workshop on Cyber Security Incident Response' hosted by Australia and Singapore, for example, explored the ability of participating States to cooperate in the event of a regional cyber security incident, focusing specifically on 'the benefits of consistent offences and information sharing mechanisms with law enforcement agencies and computer emergency response teams'.[84] Also, at the 10th ARF Security Policy Conference held in Brunei in May 2013, senior defence policy officials considered a number of cyber security cooperation opportunities, including 'the sharing of best-practices, the conducting of professional exchanges and education on cyber security, as well as streamlining efforts in enhancing cyber security between different policy areas'.[85]

However, there is evidence of a shift away from this cooperative policy in favour of a greater national cyber security focus. In the *Statement on Cooperation in Ensuring Cyber Security*, adopted at the 19th ARF on 12 July 2012, an emphasis was placed on the need to pursue measures that will 'further intensify regional cooperation on security in the use of ICTs', including through: dialogue on strategies to address cyber threats in a way 'consistent with international law'; enhanced regional cooperation in realising a 'culture of cyber security'; and the promotion of cyber 'confidence-building, stability, and risk reduction measures'.[86] Despite its common security foundations set by the 2006 Statement, this document implicitly recognises the growing correlation between cyberspace and national security concerns, hence emphasising 'confidence-building and other transparency measures' necessary to 'reduce the risk of misperception, escalation and conflict'.[87] In keeping with this growing national security concern in cyberspace, the work plan was developed in 2015 with the proposal of various confidence building measures to reduce the risk of conflict stemming from the use of ICTs.[88]

As South Korean Ambassador to the UN Conference on Disarmament, Kwon Haeryong observes, Asia-Pacific States are in general 'rather unengaged' on issues relating to the international governance of cyberspace.[89] In the ARF context, where many States' own cyber security strategies are still in their nascent form, this is unsurprising. The present and future uncertainties about the cyber security landscape and its implications for geopolitical rivalry between ARF Member States are reflected in the fundamental differences between their approaches to cyber security. These uncertainties and divergent policy approaches undermine the ARF's ability to galvanise members into collective action on cyber security.[90]

Indeed, the line of division became evident at the ARF 'Workshop on Measures to Enhance Cyber Security – Legal and Cultural Aspects' held in Beijing on 11–12 September 2013.

---

[84] 'ASEAN Regional Forum Work Plan for Counter-Terrorism and Transnational Crime 2011–2012' in *ASEAN Regional Forum at Twenty: Promoting Peace and Security in the Asia-Pacific* (World Affairs Press 2013) 214.

[85] '10th ASEAN Regional Forum Security Policy Conference' (ASEAN Summit 2013, 23 May 2013).

[86] 'Chairman's Statement of the 19th ASEAN Regional Forum' (19th ARF, Phnom Penh, Cambodia, 12 July 2012) Annex 4: 'ARF Statement on Cooperation in Ensuring Cyber Security'.

[87] Ibid.

[88] See 'ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies (ICTs)' (7 May 2015) aseanregionalforum.asean.org/wp-content/uploads/2018/07/ARF-Work-Plan-on-Security-of-and-in-the-Use-of-Information-and-Communications-Technologies.pdf accessed 31 July 2020. See also 'Chairman's Statement of the 20th ASEAN Regional Forum' (20th ARF, Bandar Seri Begawan, Brunei Darussalam, 2 July 2013) para 33.

[89] Haeryong (n 38).

[90] See Rees (n 18) 408.

Throughout the workshop, Chinese and Russian delegations referenced their jointly drafted International Code of Conduct, which maintains that 'policy authority for Internet-related public issues is the sovereign right of States'. Many Western States have criticised the code as inconsistent with international practices and instruments, including the Universal Declaration of Human Rights.[91] According to Feakin, this reflects a familiar tension in the quest to secure the cyber realm, whereby 'China and a selection of partners, including Russia, advocate a State-led legal approach, while most Western States advocate the "multi-stakeholder" approach which shies away from legally binding agreements and advocates the promotion of norms of behaviour in cyberspace'.[92] Such division of perspectives to cyber security at the fundamental level has since then cemented cyberspace as the invisible battleground of ideological warfare,[93] further restricting the ARF's ability to constructively engage in cyber confidence building.

(c) Asia-Pacific Economic Cooperation (APEC)

With a membership base consisting of 21 Pacific Rim economies, APEC is a major forum in the Asia-Pacific region. Formed in 1989, the forum's overall objectives are to promote business, trade and investment liberalisation, and economic growth and prosperity in the region.[94] In 1990, the APEC Telecommunications and Information Working Group (APEC TEL) was created, with a mission to advance 'the development of information and communication technology (ICT) infrastructure and services in the Asia-Pacific region' and to promote 'cooperation, information sharing and the development of effective ICT policies and regulations'.[95] The APEC Senior Officials and Telecommunications and Information Ministers and Leaders (TELMIN) direct and oversee the Telecommunications and Information Working Group's activities. In turn, APEC TEL, which meets biannually, operates through three steering groups: the Liberalisation Steering Group, the ICT Development Steering Group, and the Security and Prosperity Steering Group (SPSG).

Initially, APEC's engagement with the cyber realm focused on issues 'such as e-commerce, identity theft, and related developments, before shifting in the late 1990s to focus on criminal aspects of cyberspace (particularly information security)',[96] reflecting its economic focus. APEC also concentrated efforts on the regional realisation of the full socio-economic benefits of the digital age, as reflected in the Brunei Goals adopted by the APEC Leaders in 2000.[97] The

---

[91] See 'Co-Chair's Summary Report on ARF Seminar on Confidence Building Measures in Cyberspace' (Seoul, Republic of Korea, 11–12 September 2012) para 17.

[92] Tobias Feakin, 'ARF, and how to change the tune of the cyber debate', *The Strategist* (14 October 2013) https://www.aspistrategist.org.au/arf-and-how-to-change-the-tune-of-the-cyber-debate/ accessed 31 July 2020.

[93] International Institute for Strategic Studies (n 25) Ch 5; Shannon Tiezzi, 'Chinese military declares the Internet an ideological "battleground"', *The Diplomat* (21 May 2015) https://thediplomat.com/2015/05/chinese-military-declares-the-internet-an-ideological-battleground/ accessed 31 July 2020.

[94] '1989 APEC Ministerial Meeting' (Joint Statement, Canberra, Australia, 6–7 November 1989).

[95] APEC TEL, 'Telecommunications and Information' (APEC Secretariat, 2019) https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information accessed 31 July 2020.

[96] Thomas (n 35) 13 [footnotes omitted].

[97] APEC Leaders, 'Bandar Seri Begawan Declaration – Delivering to the Community' (Bandar Seri Begawan, Brunei Darussalam, 16 November 2000) paras 15–17.

'Action Agenda for New Economy',[98] adopted in the same year, envisaged the materialisation of a 'digital society',[99] and in 2001 the e-APEC Task Force expanded on it in the *e-APEC Strategy*.[100] The *e-APEC Strategy* details three cyber-focus areas, namely: creating an 'environment for strengthening market structures and institutions'; facilitating an 'environment for infrastructure investment and technology development'; and enhancing 'human capacity building and promot[ing] entrepreneurship'.[101]

The events of 9/11 precipitated a shift in APEC's dialogue on cyber issues. A little over a month after the attacks, APEC leaders issued a statement condemning international terror, noting that it posed a 'direct challenge to APEC's vision of free, open and prosperous economies, and to the fundamental values that APEC members hold'.[102] Furthermore, APEC leaders acknowledged the 'imperative to strengthen international cooperation at all levels in combating terrorism in a comprehensive manner',[103] including enhanced critical sector protection in the area of telecommunications infrastructure.[104] A year later, this time in the wake of the 'Bali bombings', the *APEC Leaders Statement on Fighting Terrorism and Promoting Growth* recognised the need for enhanced cyber security, noting that 'the global communications network is only as secure as its weakest link'.[105]

APEC's Counter Terrorism Action Plans (CTAPs), whose development stemmed from these counterterrorism statements, devote a section to 'promoting cyber security' and reaffirm commitments to 'counter…terrorism by implementing and enhancing critical information infrastructure protection and cyber security to ensure a trusted, secure and sustainable online environment'.[106] The CTAPs provide a space where member economies can record their APEC commitments to the promotion of cyber security, as well as the past and future measures they have taken/intend to take to meet these commitments. With a view to strengthening regional ICT infrastructure, the Plans also ask members to detail cyber capacity building needs and areas of cyber security expertise that might assist other APEC members.

In August 2002, the US delegation to APEC TEL submitted the APEC Cybersecurity Strategy at its 26th meeting. This document reportedly laid the foundation for the *Shanghai Declaration*,[107] in which APEC TELMIN emphasises the importance of network security and the development of IT security standards and best practice guides.[108] It also directed APEC TEL to 'give special priority to and facilitate within APEC work on the protection of informa-

---

[98] Ibid. Annex 1: 'Action Agenda for New Economy'.

[99] APEC Electronic Commerce Steering Group (ECSG), 'e-APEC Strategy' (Report, October 2001) 1 https://www.apec.org/Publications/2001/10/eAPEC-Strategy-October-2001 accessed 31 July 2020.

[100] Ibid.

[101] Ibid. 1–2. See also APEC Leaders (n 97).

[102] 'APEC Leaders Statement on Counter-Terrorism' (Shanghai, China, 21 October 2001) para 2.

[103] Ibid., para 4.

[104] Ibid., para 6.

[105] 'APEC Leaders Statement on fighting terrorism and promoting growth' (Los Cabos, Mexico, 26 October 2002).

[106] See APEC, 'Counter terrorism action plans' (APEC Secretariat, 2019) https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Counter-Terrorism/Counter-Terrorism-Action-Plans accessed 31 July 2020.

[107] APEC TELMIN5, 'Shanghai Declaration' (Shanghai, China, 29–30 May 2002).

[108] Ibid. Annex A: 'Program of Action', and Annex B: 'Statement on the Security of Information and Communications Infrastructures'.

tion and communications infrastructures'.[109] To this end, the SPSG has been working towards promoting and realising security in the cyber realm.[110] In October 2002, APEC Leaders made a commitment to enact domestic laws governing cyber security and cybercrime.[111] They also agreed that cyber-laws and policy should be consistent with international legal instruments, including the Council of Europe's *Convention on Cybercrime*,[112] and the United Nations General Assembly Resolution 55/63.[113] They supported the development of national CERTs, in order to enable the 'exchange [of] threat and vulnerability assessment'.[114]

In 2005, the APEC Senior Officials recognised in the *APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment* ('2005 Cybersecurity Strategy') that the ability of members and their citizens to harness ICT's full potential, as envisaged in the 2000 *Brunei Goals* and 2001 *e-APEC Strategy*, had become increasingly dependent on the 'integrity and security' of cyberspace.[115] They considered that cyber security sat firmly within APEC's core mandate, given that 'most traditional economic and social activities in many APEC Member Economies have become dependent on the online environment'.[116] In light of this, the 2005 Cybersecurity Strategy sought to:

- coordinate domestic legal and policy approaches to cyber threats;
- develop regional mechanisms to 'prevent cyber attacks and minimize damage and recovery time from incidents';
- enhance public cyber security awareness;
- develop cyber security partnerships across industries and sectors;
- encourage research and development into improving the security of the online environment; and
- support regional cooperation in creating a 'trusted, secure and sustainable online environment'.[117]

The goals and commitments of these core cyber security documents have formed the basis of subsequent TELMIN statements and APEC cyber strategies. In its *Strategic Action Plan: 2010–2015*, adopted by TELMIN8 in 2010, the Telecommunications and Information Working Group re-affirms its commitment to cyber security capacity development, 'including through distribution of best practice approaches, information sharing, technical cooperation,

---

[109] Ibid. Annex B.

[110] See APEC TEL, 'Security and Prosperity Steering Group' (APEC Secretariat, 2019) https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information/Security-and-Prosperity-Steering-Group accessed 31 July 2020.

[111] See APEC Leaders Statement on fighting terrorism and promoting growth (n 104).

[112] Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) CETS No. 185. On cybercrime see Kastner and Mégret (Ch 12 of this Handbook).

[113] UNGA Res 55/63 (4 December 2000) UN Doc A/RES/55/63. On the UN's approach to cyber security see Henderson (Ch 28 of this Handbook).

[114] APEC Leaders Statement on fighting terrorism and promoting growth (n 105).

[115] APEC TEL, 'APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment' (endorsed by the APEC Senior Officials, November 2005) http://www.apec.org/-/media/Files/Groups/TEL/05_TEL_APECStrategy.pdf accessed 31 July 2020.

[116] Ibid.

[117] APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment (n 115).

training and education'.[118] The *Strategic Action Plan: 2016–2020* places emphasis on the promotion of a secure, resilient and trusted ICT environment by, for example, encouraging information sharing relating to emerging cyber security threats and challenges, and approaches for managing cyber risks.[119] Building on these commitments and endorsement from the APEC Economic Leaders, the APEC Framework for Securing the Digital Economy has been developed to provide high-level principles and strategies.[120] According to these principles, APEC Leaders recognise digital security as a shared responsibility and consider that cooperation is essential to effectively manage digital security risks, which should be balanced against the danger to privacy protection.[121]

One of the striking aspects of APEC's cyber security approach is its proactive engagement with the private sector through its various workshops and training programs.[122] However, APEC's engagement with cyber security is by no means confined to private security in cyberspace. Indeed, at the opening session of the 44th meeting of APEC TEL in 2011, Malaysia raised concerns about 'negative acts' in the cyber realm that 'threaten the stability of Government'.[123] Also, in its 2012 CTAP, Mexico listed 'technical support regarding Advanced Persistent Threats against government' as a capacity building need for them. Likewise, Brunei Darussalam identified in its 2018 CTAP the lack of expertise in the areas of cybersecurity and cybercrime.[124]

APEC has also been working closely with other institutions such as the OECD, the International Telecommunications Union, and ASEAN, in many cyber security areas including 'security of information systems and networks, awareness raising, malware, the protection of children online and botnets'.[125] Through such engagement, as well as facilitating cyber cooperation between member economies at the CERT level, APEC ensures that its critical activities in the field of cyber security have 'the widest possible input and support' extending

---

[118] APEC TEL, 'Strategic Action Plan: 2010-2015' (endorsed by TELMIN8, Okinawa, Japan, 30–31 October 2010) 4. This Strategic Action Plan, along with the TELMIN8 *Okinawa Declaration*, reflect two emerging focal points for APEC's cyber security policy: cyber threats posed to vulnerable groups, particularly children; and consumer protection measures, particularly in relation to 'personal information protection': APEC TELMIN8, 'Okinawa Declaration: ICT as an engine for new socio-economic growth' (Okinawa, Japan, 30–31 October 2010) para 19; APEC TELMIN10, 'Saint Petersburg Declaration: Building confidence and security in the use of ICT to promote economic growth and prosperity' (St Petersburg, Russia, 7–8 August 2012) para 26.

[119] APEC TEL, 'Strategic Action Plan 2016-2020' (endorsed by TELMIN10, 30-31 March 2015) 5, 9. See also 'Joint Ministerial Statement' (adopted at the 2017 APEC Ministerial Meeting, Da Nang, Vietnam, 10 November 2017) para 62.

[120] APEC TEL, 'Final APEC Framework for Securing the Digital Economy' (2019/SOM1/TEL59/PLEN/020, endorsed by TEL59, Santiago, Chile, 4–7 March 2019).

[121] Ibid. paras 20–22.

[122] See Thomas (n 35) 14. For TEL cyber security projects, see APEC TEL, 'Telecommunications and Information' (APEC Secretariat, 2019) https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information accessed 31 July 2020.

[123] Ministry of Information, Communications and Culture Malaysia, 'Malaysia Urges APEC TEL to Intensify Cybersecurity Cooperation' (Press Release, 26 September 2011).

[124] See above (n 106).

[125] OECD (n 12) annex 1, 36.

its reach even to Taiwan and Hong Kong – 'two of the most networked economies in the region' – filling the gap of ASEAN-based approaches in regional security architecture.[126]

4. ASIA-PACIFIC REGIONALISM AND CYBER SECURITY

Most of the Asia-Pacific's cyber security initiatives, particularly by ASEAN and APEC, have focused upon regional cooperation in building national cyber security resilience and more comprehensive efforts to address common threats, such as the malicious cyber activities of criminal and terrorist organisations. These initiatives are consistent with the cooperative security foundation as set forth, for example, in the 2006 ARF Cyber Security Statement and the 2009 Vision Statement. However, the normative impact of such cooperative approach on Asia-Pacific regionalism has been limited in the following three areas.

First, there are marked differences in the understanding of how principles of international law are or ought to be applied in establishing the means by which the common goal of a secure and stable cyberspace can be achieved. One approach regards cyberspace as a 'free space', considering that the 'openness' of the internet should be preserved and that cyber security policies need to respect human rights, such as freedom of expression, access to information, and privacy.[127] At the another end of spectrum is a top-down governmental regulatory approach, often associated with the PRC's official cyber policy, which envisages the imposition of law and order including the ban on the use of the internet 'to incite ethnic hatred and separatism, to promote cult and to distribute salacious, pornographic, violent or terrorist information'.[128] Repeated failure to reach an agreement by the UN Group of Governmental Experts since December 2015 is, at the fundamental level, reflective of these diverging approaches and normative preferences.[129] In the Asia-Pacific, where great power rivalries are blended with political, economic, and socio-cultural diversity, such normative tension remains a serious impediment to the region's effort to develop a 'peaceful, secure and resilient rules-based cyberspace'[130]

Second, as the cyber infrastructure develops at an alarmingly rapid pace and the whole of society becomes reliant on it, some States are increasingly concerned by the potential vulnerability of their government in cyberspace.[131] This is particularly the case where information technology is used to disseminate false and misleading information against the government or

---

[126] Thomas (n 35) 14.

[127] See OECD (n 12) 4.

[128] 'ASEAN Regional Forum Annual Security Outlook' (Vol 14, 2013) 46.

[129] See, e.g., Anders Henriksen, 'The end of the road for the UN GGE Process: The future regulation of cyberspace' (2019) 5 *Journal of Cybersecurity* 1, 3–5; Michael N Schmitt and Liis Vihul, 'International cyber law politicized: The UN GGE's failure to advance cyber norms' (30 June 2017) *Just Security*, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ accessed 31 July 2020; Eneken Tikk and Mika Kerttunen, 'The alleged demise of the UN GGE: An autopsy and eulogy' (Cyber Policy Institute 2017) https://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf accessed 31 July 2020.

[130] 'ASEAN Leaders' Statement on Cybersecurity Cooperation' (adopted at the 32nd ASEAN Summit, 27 April 2018) para 5. See also 'Chairman's Statement of the 3rd ASEAN Ministerial Conference on Cybersecurity' (Singapore, 19 September 2018) para 8.

[131] See above Ministry of Information, Communications and Culture Malaysia (n 123) and accompanying text.

to otherwise undermine the legitimacy of the government. Many countries in Southeast Asia have indeed criminalised the use of information technology for disseminating information considered to be detrimental to the security of the State or perceived to be false and misleading by the government.[132] Various cyber security initiatives that have been adopted in the Asia-Pacific, with the focus on building national cyber security resilience and comprehensive efforts to address malicious cyber activities, are likely to respect and reinforce such national efforts, tipping the balance in normative preference towards tighter regulatory control of cyberspace.

Third, the increased recognition of cyberspace as the fifth domain of warfare poses challenges to the development of regional cyber security architecture. As discussed in Section 2 above, hostile or malicious use of cyberspace has the potential to amplify existing geopolitical tensions and could even trigger a spiral of conflict. It has been suggested that an expanded regional arrangement with great powers would be beneficial for the entire region, particularly in relation to cyber incidents. This is because ASEAN's perception as a 'neutral broker' positions it well to mitigate tensions arising from great power rivalries.[133] However, each State's strategic considerations, as well as different approaches to the legal regulation of cyberspace, have frustrated regional efforts to 'reduce the risk of misperception, escalation and conflict'.[134] Despite the recent developments in clarifying the applicability of international law to the conduct of States in cyberspace,[135] many of the Asia-Pacific States are yet to develop their legal response to hostile cyber activities and to appreciate its full implications for the legal relation of States in the interconnected network societies. Given all the different political interests and strategic considerations, it remains to be seen how the regional cyber security architecture might evolve to govern the conduct of States in cyberspace.

5. CONCLUSION

Since the publication of this chapter in the first edition in 2013, there has been a greater awareness of cyber security in the Asia-Pacific, with many countries adopting or renewing their national cyber security policy. During this period, regional institutions, such as ASEAN, the ARF, and APEC, have also continued to make concerted efforts to galvanise Member States and economies into collective action for the purposes of improving regional ICT infrastructure and reducing the risk of cyber intrusion and destabilisation via potential 'weak links' in

---

[132] See, e.g., Protection from Online Falsehoods and Manipulation Act 2019 (Singapore); Computer Crime Act 2017 (Thailand) s 14(2); Law on Cybersecurity (Vietnam) No 24/2018/QH14, arts 5(i), 8(1)(d).

[133] Heinl (n 36) 135.

[134] 'ARF Statement on Cooperation in Ensuring Cyber Security' (n 86) preamble para 9.

[135] Australian Government, 'Australia's International Cyber Engagement Strategy' (2017) Annex A: Australia's Position on How International Law Applies to State Conduct in Cyberspace https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf accessed 31 July 2020; 'Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace' (2019) https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html accessed 31 July 2020; 'Joint Statement by the United States of America and the Republic of Singapore' (2 August 2016) para 9 https://obamawhitehouse.archives.gov/the-press-office/2016/08/02/joint-statement-united-states-america-and-republic-singapore accessed 31 July 2020; Tallinn Manual 2.0 (n 14).

the increasingly interconnected network societies. These regional institutions have sought to prevent, regulate, and mitigate the effects of malicious use of the internet for criminal and terrorist purposes, largely through enhanced information sharing between national CERTs as well as domestic law enforcement agencies, and by setting regional standards for national cyber-related laws and policy.

However, many States have shifted their focus to national security concerns arising from strategic use of information technology. The 'openness' of cyberspace with free flow of information has increasingly been seen as posing threats to the stability of political regimes, which has led to tighter regulatory control of cyberspace at the national level. In contrast, regional efforts to develop or clarify 'rules of engagement' in cyberspace have remained stagnant despite the risk of hostile cyber activities amplifying existing geopolitical tensions in the Asia-Pacific, due to the strategic and tactical advantages that States can gain from the exploitation of cyberspace. The divergence in regulatory approach and strategic interest in the normative debate regarding the application of international law in cyberspace continues to impair the region's effort to develop a peaceful, resilient, and rules-based cyber security architecture.

28. The United Nations and the regulation of cyber-security

Christian Henderson[1]

1. INTRODUCTION

The importance of cyberspace in today's interconnected and highly complex world cannot be overstated. It has become central to the smooth running of the world economy, the carrying out of daily business transactions, political communications, as well as for social networking. The late 1990s saw an exponential growth in the use of the Internet with nearly 5 billion users across the world today.[2]

While in general the emergence of cyberspace has undoubtedly proved to be an immensely positive development, its rise has also been accompanied by a more sinister side, in that the development of information and communication technologies (ICTs) has given rise to various risks to individuals, societies and States more broadly. Although 'governments have attempted to address these issues by creating national-level mechanisms, the very transnational nature of cyberspace has forced the international community to debate and form norms or rules that should promote good behavior in cyberspace'.[3] Activity in this respect has been occurring in various institutional and regional forums for some time. For example, the Organization for Security and Co-operation in Europe (OSCE) Budapest Convention on Cybercrime entered into force in 2004 and is seen as a positive precedent in the regulation of this element of cyber-security.[4]

Activity within the UN to address cyber-security issues begun when the Russian Federation introduced a draft resolution into the UN General Assembly (UNGA) in 1998 on '[d]evelopments in the field of information and telecommunications in the context of international security'.[5] Subsequent initial activity within the UN proved somewhat 'dull without much movement … towards dealing with issues in cyberspace'.[6] Yet, 'mounting reports of disruptions and the increasing potential of cyber attacks disturbing the peace in the real world led countries to examine these challenges more seriously within the UN'.[7] Indeed, the Distributed

[1] The author wishes to thank April Longstaffe for her research assistance in preparing the first edition of this chapter. All websites last accessed on 20 September 2020.

[2] World Internet Usage and Population Statistics, Internet World Stats (30 September 2020) http://www.internetworldstats.com/stats.htm.

[3] Rahul Prakash and Darshana M Baruah, 'The UN and Cyberspace Governance' (ORF Issue Brief 86, February 2014) 1 http://orfonline.org/cms/export/orfonline/modules/issuebrief/attachments/issuebrief68_1394871027354.pdf.

[4] Convention on Cybercrime (Council of Europe), CETS No. 185, 23 November 2001 (entered into force: 1 July 2004).

[5] UNGA Res 53/70 (4 December 1998) UN Doc A/RES/53/70.

[6] Prakesh and Baruah (n 3) 1.

[7] Ibid., 1–2.

Denial of Service Attacks (DDoS) on Estonia (2007) and Georgia (2008), the Stuxnet worm attack upon Iran (2010), the Edward Snowden revelations (2013) regarding the use of ICTs by States to spy upon one another, as well as the accusation that Russia interfered in the US elections (2016) brought to light in dramatic fashion the realities of cyberspace being used in unscrupulous ways and raised the profile of cyber-security on the UN's agenda. In light of these events, it is fair to say that '[t]he issue of cyber security is quickly making its way up the agenda of global public policy issues demanding attention'.[8]

While one might, nonetheless, take the view that '[t]here has been only limited U.N. action on the issue of cyber-security',[9] this is arguably down to the fact that there have been fundamental differences on fundamental issues between Eastern and Western States. The main sticking points appear to be whether there should be a free flow of information or whether there should be governmental restrictions upon it; whether the focus should be on economic espionage and criminal activity or upon the use of cyberspace to carry out attacks; and whether, and if so how, existing international law applies to cyber-security issues or whether new rules and norms need to be developed, perhaps in the form of a new treaty. In this respect, the UN 'has been working for over a decade to eliminate these differences and create a mechanism to ensure the security and stability of cyberspace'.[10] As this chapter will attempt to highlight, the UN, through its work on both issues of cyber-warfare and cyber-crime,[11] is now moving with some momentum, albeit with some stuttering along the way.

The UN's activities in this area are highly fragmented with a very complex system of bodies dealing with it and with expertise scattered throughout the system meaning that a full analysis is beyond the limited scope of this chapter. The purpose of this chapter is thus twofold. Its primary aim is to provide an overview of UN activities and initiatives concerning the regulation of cyberspace and cyber-security. The chapter also attempts, however, to discern whether any regulatory norms have emerged in this field of activity through the UN processes. While it will touch upon issues such as the use of force in cyberspace and cyber-crime, these have been dealt with in-depth in other chapters of this Handbook.[12]

2. THE UNITED NATIONS GENERAL ASSEMBLY

While the UNGA may in several respects be considered the second organ of the UN in regard to the maintenance of international peace and security, and can only make recommendations as opposed to legally oblige States to take a particular course of action,[13] it has nonetheless

---

[8] Paul Meyer, 'Cyber security takes the floor at the UN', *opencanada.org* (12 November 2013) http://opencanada.org/features/the-think-tank/comments/cyber-security-takes-the-floor-at-the-un/.

[9] Oona A Hathaway and others, 'The law of cyber-attack' (2012) 100 *California L Rev* 817, 865.

[10] Prakesh and Baruah (n 3) 1.

[11] While there is an obvious overlap between the two, cyber-warfare is mainly concerned with how '[information] technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States' (see UNGA Res 53/70 (4 January 1999) UN Doc A/RES/53/70) while cyber-crime, on the other hand, is concerned in general with 'the criminal misuse of information technologies' (See UNGA Res 55/63 (22 January 2001) UN Doc A/RES/55/63).

[12] See Kastner and Mégret (Ch 12 of this Handbook) and Roscini (Ch 14 of this Handbook).

[13] UN Charter 1945 arts 10–17.

been central in the process of norm development in the context of cyber-security. The main discursive work of the UNGA occurs in its various committees, of which there are six.[14] Three of the UNGA's six committees have met to discuss the issue of cyber-security and negotiate draft resolutions in relation to it, which were then submitted to the plenary for adoption at the UNGA's annual session each year.

(a) The First Committee

The First Committee of the UNGA – the Disarmament and International Security Committee – is concerned with disarmament and related international security questions and was the first committee to engage with issues of cyber-security. Indeed, the issue of information security has been on the agenda of the UN since 1998 when the Russian Federation introduced its draft resolution in the First Committee on '[d]evelopments in the field of information and telecommunications in the context of international security', which was subsequently adopted without a vote.[15] This resolution built upon previous work on the '[r]ole of science and technology in the context of security, disarmament and other related fields'[16] and has been subsequently introduced every year since. Its key elements are that it:

- mentions the dual use of developments in the area and the military potential of ICTs for the first time;[17]
- expresses concern about the use of such technology 'inconsistent with the objectives of maintaining international stability and security';[18]
- noted the need for broad international cooperation;[19]
- called upon Member States to promote at multilateral levels the consideration of existing and potential threats in the field of information security;[20]
- mentions the need to prevent cyber-crime and cyber-terrorism;[21] and
- invited Member States to inform the UN Secretary-General of their views regarding 'definitions' and the development of 'international principles'.[22]

In introducing this resolution, Sergey Ivanov, Minister of Defence of the Russian Federation from 2001 to 2007, stated that 'Russia want[ed] to develop international law regimes for preventing the use of information technologies for purposes incompatible with missions of

---

[14] The six main committees of the UNGA are: First Committee (Disarmament and International Security Committee), Second Committee (Economic and Financial Committee), Third Committee (Social, Humanitarian and Cultural Committee), Fourth Committee (Special Political and Decolonization Committee), Fifth Committee (Administrative and Budgetary Committee), and Sixth Committee (Legal Committee).

[15] UNGA Res 53/70 (4 December 1998) UN Doc A/RES/53/70.

[16] UNGA 'Role of science and technology in the context of security, disarmament and other related fields' (18 November 1998) UN Doc A/53/576.

[17] UNGA Res 53/70 (n 15) preamble.

[18] Ibid.

[19] Ibid.

[20] Ibid., para 1.

[21] Ibid., preamble.

[22] Ibid., para 2.

ensuring international stability and security.'[23] However, the US has always taken, and as noted below continues to take, the position that '[t]he same laws that apply to the use of kinetic weapons should apply to state behaviour in cyberspace' while trying to increase cooperation among law enforcement agencies.[24] In this respect, the original push by Russia for what was perceived as an international treaty was met with suspicion by the US and EU States in the belief that a treaty could be used to limit the freedom of information under the guise of increasing information and telecommunications security.[25]

Yet, while the idea of an international treaty to regulate cyberspace was divisive, this did not impact upon general support for the resolution itself. Indeed, in 2005, an important change took place in the First Committee in that the draft resolution that had been introduced into the UNGA annually by Russia was adopted but went to a recorded vote.[26] The US was the only State to vote against the resolution.[27] Arguably as a result of US opposition the draft resolution introduced in 2006 was no longer sponsored by Russia alone, but also co-sponsored by China, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Myanmar, Tajikistan, and Uzbekistan.[28] Additional States joined as co-sponsors in subsequent years.[29]

However, after President Obama had succeeded President Bush as President of the United States in 2009 the US adopted a 'reset' policy not only with regards to Russia but also with the UN itself.[30] The US subsequently agreed to discuss cyber-warfare and cyber-security with representatives of the First Committee.[31] In January 2010, President Obama presented a position paper with the objective of bringing the two parties together[32] and, later that year, the US went on to reverse its long-time policy position towards the annually introduced resolution and for the first time became a co-sponsor of the draft resolution.[33] Yet, this did not mean that the US had fully aligned itself with the position of the Russian Federation. On the contrary, there were two key changes to the 2010 draft from the original draft of the resolution:

- omission of the reference to, and attempts to come up with, definitions that were perceived as a first step towards a cyber arms control treaty; and

---

[23] Christopher A Ford, 'The trouble with cyber arms control' (2010) 29 *The New Atlantis: A J of Technology and Society* 52, 65.

[24] Ibid., 67.

[25] China was initially relatively quiet on this issue but subsequently appeared to align itself with the position of Russia.

[26] See UNGA 'Developments in the field of information and telecommunications in the context of international security: Report of the First Committee' (16 November 2005) UN Doc A/60/452.

[27] Ibid.

[28] See UNGA Developments in the field of information and telecommunications in the context of international security – Armenia, Belarus, China, Kazakhstan, Kyrgyzstan, Myanmar, Russian Federation, Tajikistan and Uzbekistan: draft resolution' (11 October 2006) UN Doc A/C.1/61/L.35.

[29] UNGA 'Developments in the field of information and telecommunications in the context of international security: Report of the First Committee' (9 November 2006) UN Doc A/61/389.

[30] Tim Maurer, 'Cyber norm emergence at the United Nations: An analysis of the activities of the UN regarding cyber-security' (Belfer Center for Science and International Affairs, Discussion Paper #2011–11 September 2011) 23 http://belfercenter.hks.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

[31] Ibid.

[32] Ibid.

[33] Ibid., 24.

- substitution of the reference to 'international principles' with references to what was perceived as more benign language in the form of 'international concepts' and 'possible measures'.

While the resolution, albeit with certain amendments,[34] continues to be introduced in the UNGA each year, the main work of the First Committee and the focus of its resolutions has centred on the work of several Groups of Governmental Experts (GGEs), which will be addressed below. Before doing so, it should not be forgotten that work on the issue of cyber-security has also been undertaken in the Second and Third Committees of the UNGA.

(b) The Second Committee

The Second Committee – the Economic and Financial Committee – is concerned with economic questions, so might not immediately be seen to be relevant in discussions regarding cyber-security. However, while it is fair to say that the First Committee has tended to focus upon issues of cyber-warfare and the Third Committee upon issues of cyber-crime,[35] the Second Committee has addressed both through its 'Global Culture of Cyber-security' initiative. The three resolutions of the UNGA's Second Committee on this initiative are concerned with both cyber-warfare and cyber-crime and all reference the resolutions of both the First and Third Committees.[36]

In light of the decision of the Third Committee to no longer focus on cyber-crime, the US introduced a new draft resolution in the Second Committee in 2002 entitled '[c]reation of a global culture of cyber-security'. While initially co-sponsored by Japan, Australia and Norway, after a number of revisions to the original draft 36 other Member States joined as co-sponsors, including the Russian Federation.[37] Indeed, one of the revisions was to introduce references to resolutions adopted within the UNGA's First Committee, which had, as noted above, been mainly drafted by Russia. It was subsequently adopted without a vote.[38]

There were several significant elements to this original resolution. First, in order to attract the support of many developing countries the resolution had a focus on capacity building, which was something that the GGEs subsequently set much store by.[39] The preamble noted, for example, that 'gaps in access to and the use of information technologies by States can diminish the effectiveness of international cooperation in combating the criminal use of information technology' while the final operative paragraph '[s]*tresse*[d] the necessity to facilitate the transfer of information technology and capacity-building to developing countries, in order

---

[34] For example, the inclusion of references to the importance of respect for human rights and fundamental freedoms in the use of information and communications technologies, the need to address threats consistent with the free flow of information, and references to the various initiatives of the UN Secretary-General and the responses of Member States.

[35] See sections 2(a) and 2(c) of this chapter respectively.

[36] UNGA Res 57/239 (31 January 2003) UN Doc A/RES/57/239; UNGA Res 58/199 (30 January 2004) UN Doc A/RES/58/199; UNGA Res 64/211 (17 March 2010) UN Doc A/RES/64/211.

[37] UNGA 'Macroeconomic policy questions: science and technology for development: Report of the Second Committee' (21 December 2002) UN Doc A/57/529/Add.3. China did not co-sponsor the resolution.

[38] UNGA Res 57/239 (n 36).

[39] See section 2(d) of this chapter.

to help them to take measures in cybersecurity'.[40] Secondly, the resolution had annexed to it a series of '[e]lements for creating a global culture of cybersecurity', which Member States were invited to take into account.[41] These elements covered nine areas: awareness; responsibility; response; ethics; democracy; risk assessment; security design and implementation; security management; and reassessment.[42] While these were titled 'principles', as opposed to 'elements', in the original draft, along with the fact that they were originally due to be 'adopted' but which was later changed so that Member States were to simply take them 'into account', they nonetheless arguably represented a certain consensus regarding regulatory norms in the context of cyber-security.[43]

These 'elements' were expanded upon in the second resolution of the Second Committee on the creation of a global culture of cyber-security, that was adopted by the UNGA in January 2005, with the addition of the 'protection of critical information infrastructures'.[44] These elements included actions such as having emergency networks regarding cyber-vulnerabilities, threats and incidents,[45] examining information infrastructures and the interdependencies between them,[46] promoting partnerships, including the sharing of information, between public and private stakeholders,[47] having adequate substantive and procedural laws and trained personnel to enable effective investigations and prosecutions in response to attacks,[48] and engaging in international cooperation to secure critical information infrastructures.[49] The resolution, and the included elements, was co-sponsored by 69 countries, this time including China but not Russia.[50] Nonetheless, the broadening of the elements could be perceived as a progressive step towards the formation of a regulatory cyber-security regime.[51]

The final resolution was adopted in 2010 after the US policy shift.[52] It was sponsored by the US on behalf of 39 States, although not Russia or China. This resolution was entitled the '[c]reation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures' and included an annex outlining a '[v]oluntary self-assessment tool for national efforts to protect critical information infrastructures'. This is explained as 'a voluntary tool that may be used by Member States, in part or in its entirety, if and when they deem appropriate, in order to assist in their efforts to protect their critical information infrastructures and strengthen their cybersecurity'.[53] These include '[t]aking stock of cybersecurity needs and strategies', '[s]takeholder roles and responsibilites', '[p]olicy processes and participation', '[p]ublic-private cooperation', '[i]ncident management and recov-

---

40 UNGA Res 57/239 (n 36) para 5.
41 Ibid., para 3.
42 Ibid., appendix.
43 Maurer (n 30) 44.
44 UNGA Res 58/199 (n 36). See appendix for the expanded elements.
45 Ibid., annex, element 1.
46 Ibid., annex, element 3.
47 Ibid., annex, element 4.
48 Ibid., annex, element 9.
49 Ibid., annex, element 10.
50 UNGA 'Macroeconomic policy questions: science and technology for development: Report of the Second Committee' (15 December 2003) UN Doc A/58/481/Add.2.
51 Maurer (n 30) 44.
52 UNGA Res 64/211 (n 36).
53 Ibid., n.2.

ery', '[l]egal frameworks', and '[d]eveloping a global culture of cybersecurity'.[54] Notably, these highlight the importance of cooperation among States, including through 'international information-sharing and collaboration'.[55]

(c) The Third Committee

The Third Committee – the Social, Humanitarian and Cultural Committee – is, as its title suggests, concerned mainly with social and humanitarian issues, but in the context of cyber-security with cyber-crime. Two years after the Russian Federation introduced its resolution in the First Committee in 1998 the Third Committee discussed a draft resolution introduced by the US and 38 other States entitled '[c]ombating the criminal misuse of information technologies'.[56] It was co-sponsored by the Russian Federation, but not China, with a further 19 Member States subsequently co-sponsoring it and was adopted without a vote on 22 January 2001.[57]

The key objective of this resolution was to establish a 'legal basis for combating the criminal use of information technologies'.[58] In attempting to realize this objective, the resolution, amongst other things, noted the value of ten measures to combat the criminal misuse of information technologies including, for example, eliminating safe havens for those who criminally misuse information technologies[59] and the preservation of the capacity of governments to fight such criminal misuse.[60]

In 2001, a follow-up resolution – again, entitled '[c]ombating the criminal misuse of information technologies' – was introduced by the US and 73 other Member States, again including the Russian Federation but not China, with eight Member States joining later, and was adopted without a vote on 23 January 2002.[61] This took note of the measures set forth above, and again invited Member States to take them into account in their efforts to combat the criminal misuse of information technologies.[62]

The Third Committee adopted a resolution in 2013 entitled '[t]he right to privacy in the digital age'.[63] The Edward Snowden revelations earlier in the year were a key reason for the adoption of this resolution. It was in this sense no surprise that its two key sponsors were Brazil and Germany, the leaders of which were the main victims of NSA surveillance operations. While it was first thought that the response of these two States would be 'an initiative on the international security front at the UN, in the end, Brazil and Germany decided it was best to present the matter in the context of respect for international human rights law and the right to privacy in particular'.[64] In this regard, the resolution emphasizes that 'illegal surveillance of communications, their interception and the illegal collection of personal data constitute

---

54 Ibid., annex.
55 Ibid., preamble.
56 UNGA A/55/593 (16 November 2000).
57 UNGA 55/63 (4 December 2000) UN Doc A/RES/55/63.
58 UNGA A/57/529/Add.3 (n 37).
59 UNGA A/RES/55/63 (n 57) para 1(a).
60 Ibid., para 1(j).
61 UNGA Res 56/121 (19 December 2001) UN Doc A/RES/56/121.
62 Ibid., para 2.
63 UNGA Res 68/167 (18 December 2013) UN Doc A/RES/68/167.
64 Meyer (n 8).

a highly intrusive act that violates the right to privacy and freedom of expression and may threaten the foundations of a democratic society'.[65] The resolution recalls the obligation of States to 'ensure that measures taken to counter terrorism comply with international law' and recalls the privacy provisions of the International Covenant on Civil and Political Rights as well as the Universal Declaration of Human Rights.[66] The resolution calls upon States 'to take measures to put an end to violations of those rights'[67] and, in doing so, 'establish independent national oversight mechanisms capable of ensuring transparency and accountability of state surveillance of communications, their interception and collection of personal data'.[68] This resolution set the tone for subsequent resolutions to be adopted by the UNGA on this issue on a regular basis

At the UNGA's 73rd session in 2018 a Russian-tabled resolution on 'Countering the use of information and communication technologies for criminal purposes' was also adopted,[69] although with opposition to it from many States, including the US, Australia, Canada and the EU. The broadly worded resolution might be seen as duplicating work that is being undertaken elsewhere in the UN,[70] but also as an attempt to create a new global treaty on cybercrime. This latter concern of many States was realized the following year when this process was initiated, when the UNGA adopted a resolution in which it '*Decide[d]* to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes'.[71] The ad hoc committee is due to meet for the first time in August 2020, where it will agree and outline the modalities for its further activities.[72]

(d) The Groups of Governmental Experts

Overall, and as demonstrated by the above sections, the UNGA has been active in regards to discussing principles, elements, good practice, etc., regarding the behaviour of Member States in the context of cyber-security. However, what the above also arguably shows is that '[a]t the multilateral level, the UN [would] have to begin to address the cyber security issue in a more coherent fashion. The General Assembly [could] ill afford to have two deliberative streams (i.e. the First and Third Committee) acting in ignorance of one another'.[73] Indeed, '[t]he airing of declaratory policy at the annual General Assembly sessions should not substitute for purposeful action by states in more operational forums to tackle the pressing problems raised by destabilizing state conducted cyber operations'.[74] In this respect, the establishment of several Groups of Governmental Experts (GGE) has been a significant development. Six GGEs and an open-ended working group have been established since 2004 that have examined the existing

---

65 UNGA A/RES/68/167 (n 63) preamble.
66 Ibid.
67 Ibid., para 4(b).
68 Ibid., para 4(d).
69 UNGA A/RES/73/187 (17 January 2018).
70 See section below on the Commission on Crime Prevention and Criminal Justice and its Open-Ended Intergovernmental Expert Group on Cybercrime.
71 UNGA A/RES/74/247 (27 December 2019) para 2.
72 Ibid., para 3.
73 Ibid.
74 Ibid.

and potential threats from the cyber-sphere and possible cooperative measures to address them. The purpose of this section is to give an overview of the work of these groups.

(i) The First Group of Governmental Experts

The first GGE was established in 2004 by the UNGA's First Committee. The previous year, following on from a proposal by Russia,[75] Member States had:

> Request[ed] the Secretary-General to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them, and to conduct a study on [relevant international concepts aimed at strengthening the security of global information and telecommunications systems], with the assistance of a group of governmental experts, to be established in 2004, appointed by him on the basis of equitable geographical distribution and with the help of Member States in a position to render such assistance, and to submit a report on the outcome of the study to the General Assembly at its sixtieth session.[76]

Over the course of three meetings the GGE, which consisted of 15 members, failed to find even the smallest common denominator. It is perhaps quite unusual for such an outcome to occur at the UN where an activity is usually only initiated when it is clear before it starts that there is at least some smallest denominator that everyone can agree on.[77] However, the UN Secretary-General concluded in 2005 that it was due to 'the complexity of the issues involved' that 'no consensus was reached on the preparation of a final report'.[78]

A member of the Russian delegation at the GGE meetings claimed that '[t]he main stumbling block was the question of whether international humanitarian law and international law sufficiently regulate the security aspects of international relations in cases of "hostile" use of ICTs for politicomilitary purposes'.[79] The issue of whether existing law sufficiently regulated cyber-threats is, as noted above, something that was an issue between Russia and the US. While Moscow urged the development of new norms and rules Washington was of the opinion that 'the law of armed conflict and its principles of necessity, proportionality and limitation of collateral damage already govern the use of such technologies'.[80] Furthermore, the group was not able to agree on whether the discussions should focus on 'information content or information infrastructures',[81] with the US and EU, as noted above, suspicious of the motives

---

[75] Russia noted in its report to the UN Secretary-General that 'the group will give the international community a unique opportunity to examine the entire range of issues involved'. UNGA 'Developments in the field of information and telecommunications in the context of information security: Report to the Secretary General' (17 September 2003) UN Doc A/58/373.

[76] UNGA Res 58/32 (8 December 2003) UN Doc A/RES/58/32 para 4. The eventual GGE consisted of governmental experts from 15 States: Belarus, Brazil, China, France, Germany, India, Jordan, Malaysia, Mali, Mexico, the Republic of Korea, Russia, South Africa, UK, and US. They unanimously elected Andrey V Krutskikh of Russia as its Chairman.

[77] Maurer (n 30) 22.

[78] UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General' (5 August 2005) UN Doc A/60/202, 2.

[79] Maurer (n 30) 22.

[80] UNGA 'Developments in the field of information and telecommunications in the context of information security: Report to the Secretary General' (28 December 2004) UN Doc A/59/116/Add.1.

[81] 'Fact Sheet – Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations Office for Disarmament Affairs' http://unoda-web.s3.amazonaws.com/wp-content/uploads/2013/06/Information_Security_Fact_Sheet.pdf.

of Russia, more specifically that it was attempting to limit the freedom of information under the guise of increasing information and telecommunications security.

However, despite the lack of agreement, 'the work of the GGE was not in vain as it successfully raised the profile of the relevant issues on the international agenda'.[82] In addition, despite its notable failure the first GGE had initiated a certain momentum within the UN to consider cyber security. As such, during the 60th session of the UNGA, when the first GGE had been due to report, Member States adopted a resolution in which they:

> Request[ed] the Secretary-General, with the assistance of a group of governmental experts, to be established in 2009 on the basis of equitable geographical distribution, to *continue* to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as the [relevant international concepts aimed at strengthening the security of global information and telecommunications systems], and to submit a report on the results of this study to the General Assembly at its sixty-fifth session.[83]

The momentum that had developed as a result of the GGE initiative could only be increased by the fact that between the adoption of the resolution in 2005 requesting the establishment of a second GGE and its actual establishment in 2009 cyber-warfare had begun to make the headlines, with the DDoS attack against Estonia in 2007 and then, in 2008, with cyber-conflict issues during the Georgian-Russian war.[84] Yet, these events did not mean that agreement amongst the second group of experts was assured. On the contrary, given the intensity of the situations and the parties involved things might equally have gone the other way. As it happened, however, a consensus began to emerge within the group with the inclusion in its report of some progressive steps.

(ii) The Second Group of Governmental Experts

Given the intervening events it was interesting that Estonia was a member of the second GGE,[85] having been the first State to suffer a massive DDoS attack. The GGE, first convening in November 2009, issued the first successful report of a GGE in July 2010.[86] It is clear that with the issuance of this report the UN took 'a step forward' in its regulation of cyber-security.[87] In coming to a consensus the group was of the view that '[e]xisting and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century'.[88] Indeed, the threat was considered significant enough to pose a threat to 'international

---

[82] Maurer (n 30) 22.

[83] UNGA Res 60/45 (8 December 2005) UN Doc A/RES/60/45 para 4 [emphasis added].

[84] It is perhaps worth noting that the classification of these two incidents as examples of 'cyber-warfare' is not absolutely certain and is still dependent to an extent on the emerging consensus as to how to classify such incidents. See, in general, Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013).

[85] The eventual GGE consisted of governmental experts from 15 States: Belarus, Brazil, China, Estonia, France, Germany, India, Israel, Italy, Qatar, the Republic of Korea, Russia, South Africa, UK, and US. Mr. Andrey V Krutskikh (Russia) was unanimously elected to Chair the Group.

[86] UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General' (30 July 2010) UN Doc A/65/201.

[87] Hathaway and others (n 9) 49.

[88] UN Doc A/65/201 (n 86) 2.

peace and national security'.[89] It recalled some of the existing efforts to combat the criminal use of information technology and noted the intention to create a 'global culture of cyber security'.[90]

In adding some flesh to the bones of this statement the report highlighted the 'dual use' character of cyberspace,[91] and also acknowledged the attribution problem in connection with cyber-attacks.[92] Given the impasse between the US and the Russian Federation with regard to the utility of existing international law in addressing cyber-security or whether further rules and norms should be developed, it was perhaps of no surprise that the report failed to make an explicit reference to international law and equivocally noted that '[e]xisting agreements include norms relevant to the use of ICTs by States' although '[g]iven the unique attributes of ICTs, additional norms could be developed over time'.[93]

Arguably the most significant development in the report of the second GGE, however, were the five recommendations it made 'for the development of confidence-building and other measures to reduce the risk of misperception resulting from ICT disruptions'[94]:

- dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructures;
- confidence-building, stability, and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict;
- information exchanges on national legislation, national ICT security strategies and technologies, policies and best practices;
- identification of measures to support capacity-building in less developed countries; and
- the elaboration of common terms and definitions in connection with information security.

With these recommendations, the GGE had begun to cement four progressive themes of an emerging regulatory framework for cyber-security within the UNGA: common understandings of acceptable State behaviour, practical cooperation, confidence-building measures, and capacity-building measures. Though perhaps vague, and as the UN Secretary-General noted the international community had 'only begun to develop the norms, laws and modes of cooperation needed',[95] 'these recommendations represent[ed] real progress in overcoming a long impasse between the US and Russia over how to address cyber-security issues. The cooperation may even suggest possibilities for a future multilateral treaty under the auspices of the UN which Russia has been advocating for some time'.[96]

However, in 2010, the year in which the report had been issued and during which time the major WikiLeaks releases occurred and the Stuxnet attack against Iran had begun to unfold, a further important turning point arose in enabling the work of the UN to progress further and, in particular, establish further cooperation and normative understandings. Indeed, as noted above, it was at this point that the US decided to engage with other States to address the con-

---

89 Ibid.
90 Ibid., 7. For more on this concept see section 2(b) above on the work of the Second Committee.
91 Ibid., 6.
92 Ibid.
93 Ibid., 8.
94 Ibid.
95 UN Doc A/65/201 (n 86) 4.
96 Hathaway and others (n 9) 50.

cerns it had over cyberspace and, in particular, for the first time to co-sponsor the Russian draft resolution in the First Committee.[97] Overall, the US's 'support of the UN Resolution of 2009 (co-sponsored with Russia) as well as the successful completion of the second GGE were signs indicating this change'.[98] Furthermore, and in an attempt to build upon the substantial progress made in the report of the second GGE, the 2010 version of the resolution also included a new request to the Secretary-General to establish a further GGE in 2012 which was to submit a report at the 68th session of the UNGA in 2013.[99]

(iii) The Third Group of Governmental Experts

The third GGE was tasked with building upon the assessments and recommendations contained in the report of the second GGE and continuing to study existing and potential threats in the sphere of information security and possible cooperative measures to address them,[100] and issued its report on 7 June 2013.[101]

Forming a backdrop to the meetings of the GGE, in 2011 China, Russia, Tajikistan and Uzbekistan requested the UN Secretary-General to distribute to the 66th Session of the UNGA an International Code of Conduct for Information Security which they had drafted, and which was an attempt to provide further regulation to cyber-norms and governance.[102] In describing this document, China stated that it was 'a series of basic principles of maintaining information and network security which cover the political, military, economic, social, cultural, technical and other aspects'.[103] The Code suggested creating a multilateral mechanism in the form of a treaty to govern the Internet, something which, as noted above, had been vehemently opposed by the US. In response to the distribution of the Code of Conduct the US commented that '[a]t its heart, it calls for multilateral governance of the Internet that would replace the multistakeholder approach, where all users have a voice, with top-down control and regulation by states'.[104]

---

[97] UNGA Res 65/41 (8 December 2010) UN Doc A/RES/65/41. The resolution was sponsored by three dozen countries including China.

[98] Prakesh and Baruah (n 3) 4.

[99] UNGA A/RES/65/41 (n 97) para 4. Again, in 2011 the UNGA unanimously approved a resolution calling for a follow up to the last GGE (See UNGA Res 66/24 (2 December 2011) UN Doc A/RES/66/24).

[100] The following Member States participated in the GGE: Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, UK and USA. Ms Deborah Stokes (Australia) was unanimously elected to Chair the Group.

[101] UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General' (24 June 2013) UN Doc A/68/98.

[102] UNGA 'Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General' (14 September 2011) UN Doc A/66/359, see appendix.

[103] 'China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations' (Foreign Ministry of People's Republic of China, 13 September 2011) http://nz.chineseembassy.org/eng/zgyw/t858978.htm.

[104] Statement by Delegation of the United States of America, 'Other Disarmament Issues and International Security Segment of Thematic Debate in the First Committee of the Sixty-seventh Session of the United Nations General Assembly' (2 November 2013) http://www.state.gov/t/avc/rls/200050.htm.

The Code reflected the concerns of its sponsor States, in particular it restricted its signatories from using 'ICTs including networks to carry out hostile activities or acts of aggression and pose threats to international peace and security. Not to proliferate information weapons and related technologies'.[105] However, the US was of the opinion that:

> the draft Code appears to propose replacing existing international law that governs the use of force and relations among states in armed conflict with new, unclear, and ill-defined rules and concepts. Indeed, one of the primary sponsors of the draft Code has stated repeatedly that long-standing provisions of international law, including elements of jus ad bellum and jus in bello that would provide a legal framework for the way that states could use force in cyberspace, have no applicability. This position is not justified in international law and risks creating instability by wrongly suggesting the Internet is an ungoverned space to which existing law does not apply.[106]

Furthermore, the Code suggested 'that policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities for international Internet-related public policy issues'. The Code contained clauses curbing 'dissemination of information which incites terrorism, secessionism, extremism or undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment'.[107] However, the US was clear that:

> the introduction of a draft Code of Conduct for Information Security presented an alternative view that seeks to establish international justification for government control over Internet resources.… It would legitimize the view that the right to freedom of expression can be limited by national laws and cultural proclivities, thereby undermining that right as described in the Universal Declaration on Human Rights.[108]

Ultimately, there was little support for the draft Code of Conduct which had little impact upon the report of the third GGE. However, the third GGE 'made significant progress on agreeing on some of the defining aspects' of cyber-security.[109] As with the report of the second GGE and resolutions of the three committees of the UNGA, the report again noted the immense benefits brought by ICTs but also recognized their dual-use capabilities in that they could be used 'for purposes that are inconsistent with international peace and security'.[110] Similarly, it again noted the problem whereby the actors involved 'often act with impunity' and their malicious use of ICTs 'is easily concealed and attribution to a specific perpetrator can be difficult'.[111]

The report then focused on building upon the four progressive themes of the emerging regulatory framework for cyber-security within the UNGA: practical cooperation, common understandings of acceptable State behaviour, confidence-building measures, and capacity-building measures, and offered recommendations in respect to each including the important role of the private sector and civil society in any efforts. Where perhaps the report made most progress, however, was in its recommendations on 'norms, rules and principles of responsible behavior

---

105 International Code of Conduct for Information Security (n 103).
106 Statement by Delegation of the United States of America (n 104).
107 International Code of Conduct for Information Security (n 103).
108 Statement by Delegation of the United States of America (n 104).
109 Prakesh and Baruah (n 3) 5.
110 UN Doc A/68/98 (n 101) 6.
111 Ibid.

by States'. It was first noted that '[t]he application of norms derived from *existing* international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability'.[112] This was important, given the debate noted above between the US and the Russian Federation on this issue. If the report had left it at that question marks would have remained over what the GGE had meant when it referred to 'existing international law'. However, it went on to note that 'international law and in particular the United Nations Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment'.[113] This affirmation of the UN Charter, and perhaps in particular its rules on the non-use of force and self-defence, was significant. As the report noted further, 'State sovereignty and the international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory'.[114]

On this subject, the report was also clear that 'State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments.'[115] This was a significant step that allayed some of the fears of Western States with regard to attempts by certain States to curb free use of the Internet. Lastly on the subject of the applicability of existing international law the report noted that 'States must meet their international obligations regarding internationally wrongful acts attributable to them.'[116]

However, the report was clear that further work was needed in this context. Indeed, it stressed, again, that '[c]ommon understandings on *how* such norms shall apply to State behavior and the use of ICTs by States requires further study'.[117] What was also notable was its recognition that '[g]iven the unique attributes of ICTs, additional norms could be developed over time', something which was arguably attributable to the efforts of some States to do just that.[118]

In his forward to the new report, the UN Secretary-General noted the 'broad recognition that misuse [of ICTs] poses risks to international peace and security'. However, he also specifically:

> appreciate[d] the report's focus on the centrality of the Charter of the United Nations and international law as well as the importance of States exercising responsibility. The recommendations point the way forward for anchoring ICT security in the existing framework of international law and understandings that govern State relations and provide the foundation for international peace and security.[119]

---

[112] Ibid., 8 [emphasis added].

[113] Ibid.

[114] Ibid.

[115] Ibid. Later that year the UNGA adopted a resolution on 'the right to privacy in the digital age' which recognised the 'global and open nature of the Internet' and that 'the same rights that people have offline must also be protected online'. See UNGA Res 68/167 (21 January 2014) UN Doc A/RES/68?167.

[116] Ibid.

[117] Ibid [emphasis added].

[118] Ibid.

[119] Ibid., 4. The centrality of the UN Charter in this context has also been noted by several commentators: 'At the heart of the system is the UN Charter. It provides the legal framework which is the most accurate way to conceptualize the relationships between its various entities'. See Maurer (n 30) 12.

On 27 December 2013, the UNGA unanimously adopted a resolution in which it took note of the outcome of the third GGE, although did not specifically reiterate the conclusion that existing international law applies to cyberspace.[120] It also requested the Secretary-General to establish a further GGE that would report to the UNGA in 2015 and would study, in addition to threats and cooperative measures, the issues of the use of ICTs in conflicts and how exactly international law applies to State use of these technologies. However, it is arguably the case that 'as the mandate of the group [became] more specific it [would] increasingly be challenged to find enough common ground on which to base a consensual report that adds value to what [had] already been produced'.[121]

(iv) The Fourth Group of Governmental Experts

The fourth GGE, with an expanded 20 experts, had its first meeting in New York in July 2014 and, in July 2015, adopted a consensus report.[122] Some have expressed the view that this report added nothing significant to the 'landmark report' of the previous GGE,[123] and the 'report reaffirms the bulk of the findings of the 2013 GGE without significantly furthering understandings of how international law applies to state conduct' so that '[t]he language is largely a restatement of the earlier report adding only a few additional points.'[124] To an extent this is true. For example, the report, as with the 2013 report, broadly affirms that the UN Charter 'applies in its entirety'.[125] However, it noted the 'inherent right of States to take measures consistent with international law and as recognized in the Charter'.[126] While the report did not again explicitly state that States have a right of self-defence against cyber attacks, it could not have come much closer to doing so, in particular with its affirmation of the 'inherent right' of States to act under the Charter which could be interpreted as a reference to the right of self-defence as contained within Article 51. The report did not, however, address more specific issues, such as whether States are restricted to defending themselves through cyber-means, or whether they may resort to those of a non-cyber nature. It did note again, however, that there was a 'need for further study on the matter'.[127]

Similarly, while the report did not explicitly state that international humanitarian law applied to cyber activities, it did make reference to 'the principles of humanity, necessity, proportionality and distinction',[128] which constitute the core principles of this branch of international law. Furthermore, while it stated, as in the 2013 report, that States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms,[129] it also made reference to the UN resolutions on the right to privacy and freedom

---

120 UNGA Res 68/243 (27 December 2013) UN Doc A/RES/68/243.

121 Meyer (n 8).

122 UNGA Res 70/174 (22 July 2015) UN Doc A/RES/70/174.

123 Adam Segal, 'The UN's Group of Governmental Experts on Cybersecurity', Council on Foreign Relations, 13 April 2015, https://www.cfr.org/blog/uns-group-governmental-experts-cybersecurity.

124 Elaine Korzak, 'International Law and the UN GGE Report on Information Security' (2 December 2015) *Just Security*, https://www.justsecurity.org/28062/international-law-gge-report-information-security/.

125 UN Doc A/RES/70/174 (n 122) art 28(c).

126 Ibid.

127 Ibid.

128 Ibid., art 28(d).

129 Ibid., art 28(b).

of expression in the digital age.[130] The report also noted, however, that States have sovereignty over ICT infrastructures located upon their territory,[131] and that they must observe the principles of sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of States.[132] In this light, it was also significant that the report made a reference to the obligation of States not to 'use proxies to commit internationally wrongful acts using ICTs'[133] and to 'ensure that their territory is not used by non-State actors to commit such acts'.[134]

While the report elaborated upon – and in some ways developed – the findings of the previous two reports in respect to how international law applies to the use of ICTs, it also set forth other voluntary, non-binding norms of responsible State behaviour that 'aimed at promoting an open, secure, stable, accessible and peaceful ICT environment'.[135] These included 'cooperat[ing] in developing and applying measures to increase stability and security in the use of ICTs',[136] 'prevent[ing] ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security',[137] refraining from 'conduct[ing] or knowingly support[ing] ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public'.[138] While there was a distinction made in the report between applicable 'norms, rules and principles' and 'international law', the distinction was not often clear cut. Finally, the report proposed several confidence-building measures with the aim of strengthening security and stability in cyberspace, such as '[p]rovid[ing] assistance and training to developing countries to improve security in the use of ICTs',[139] '[a]ssist[ing] in providing access to technologies deemed essential for ICT security',[140] and '[f]acilitat[ing] cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders'.[141]

Ultimately, although there was certainly room to be sceptical as to how much was achieved in the report of the fourth GGE, the fact that the GGE had again reiterated, and in some cases expanded upon, the applicable rules and norms of international law was noteworthy and was not just of semantic value. Yet, while the report explicitly titled a section 'how' international law applies, no further guidance was given with regard to its implementation.[142] Indeed, despite the fact that '[t]he 2015 report was able to keep the interstate conversation on the reg-

---

130 Ibid., art 13(e).
131 Ibid., art 28(a).
132 Ibid., art 28 (b). Interestingly, in May 2018 the UK, although of the view that international law applied generally, rejected the existence of a rule of international law prohibiting the violation of another State's sovereignty. See https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
133 Ibid., art 28(e).
134 Ibid., art 13(c).
135 Ibid., art 13.
136 Ibid., art 13(a).
137 Ibid., art 13(a).
138 Ibid., art 13(f).
139 Ibid., art 21(b).
140 Ibid., art 21(c).
141 Ibid., art 21(e).
142 Korzak (n 124).

ulation of cyberspace on track' the 'discussions had not been easy and a number of important issues were notably absent from the consensus report'.[143]

What was of significance, however, was that when the report was endorsed by the UNGA on 30 December 2015,[144] the language of the resolution on this occasion was different and notably stronger than had been used by the UNGA upon the adoption of previous GGE reports.[145] Whereas the UNGA had previously 'taken note' of the GGE outcome reports, in 2015 it 'call[ed] upon' member States 'to be guided in their use of information and communications technologies by the 2015 report'. While the report still remains non-binding upon member States, the shift in language 'demonstrate[d] the incremental but increasing importance of the GGE process and outcome'.[146]

(v) The Fifth Group of Governmental Experts

Upon the adoption of the report of the fourth GGE, and with the aim of adding clarity to the regulation of cyberspace and cybersecurity, a fifth GGE comprising of experts from over 25 States was established in December 2015 which was due to meet during 2016-17.[147] The Group was specifically tasked by the UNGA to:

> continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them and how international law applies to the use of information and communications technologies by States, as well as norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building and the [further examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems].[148]

In what was seen as a sharp departure from the three previous GGEs that had made at least some progress since 2010, in June 2017 the GGE ended without agreement on a draft for a consensus report, with the main difficulty being the issue of international law and its application to cyberspace. The US, on the one hand, wished to see 'clear and direct statements on how certain international law applies to states' use of ICTs',[149] including, and what would be a development from the previous GGE, international humanitarian law, the right to self defence, as well as international law of State responsibility and countermeasures. This would, according to the US, 'help reduce the risk of conflict by creating stable expectations of how states may and may not respond to cyber incidents they face'.[150]

---

[143] Anders Henriksen, 'The end of the road for the UN GGE process: The future regulation of cyberspace' (2019) 5 *Journal of Cybersecurity* 1, 3.

[144] UNGA Res 70/237 (30 December 2015) UN Doc A/RES/70/237.

[145] Elaine Korzak, 'Cybersecurity at the UN: Another year, another GGE' (10 December 2015) *Lawfare*, https://www.lawfareblog.com/cybersecurity-un-another-year-another-gge.

[146] Ibid.

[147] UN Doc A/Res/70/237 (n 144).

[148] Ibid., para 5.

[149] United States Mission to the United Nations, Explanation of Position at the Conclusion of the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, New York, 23 June 2017.

[150] Ibid.

On the other hand, however, Cuba joined Russia and China's call for an 'international legally binding instrument'.[151] It was also explicit in not accepting the draft but also its reasons for doing so, in particular its concerns regarding 'the pretension of some … to convert cyber-space into a theater of military operations and to legitimize, in that context, unilateral punitive force actions, including the application of sanctions and even military actions by States claiming to be victims of illicit use of ICTs'.[152] It was clear that Cuba was not comfortable with the draft report's references to the potential applicability of the right to self-defence, the general international law principles of countermeasures and international humanitarian law.[153]

In regards to the right of self-defence, the Cuban representative objected to statements in the draft report that supposedly sought to 'establish equivalence between the malicious use of ICTs and the concept of "armed attack", as provided for in Article 51 of the Charter, which attempts to justify the alleged applicability in this context of the right to self-defense.'[154] This would constitute, it was argued, a 'fatal blow to the collective security and peacekeeping architecture established in the Charter of the United Nations', essentially turning the field into the 'Law of the Jungle', in 'which the interests of the most powerful States would always prevail to the detriment of the most vulnerable'.[155] While there was perhaps some justification for these objections, particularly given the arguably disproportionate focus of both some States and scholars on the applicability of international law and the right of self-defence to grave and serious cyberattacks,[156] with less – and arguably more warranted – focus on 'below the use of force threshold' attacks/operations 'that consist of various forms of espionage, manipulation of data, criminal activities and different and novel forms of coercion that cause little physical destruction',[157] they were also made in light of the reports of the previous GGEs which had already noted the application of the UN Charter in its entirety to cybersecurity.[158]

The Cuban representative also highlighted the draft report's references to the law of armed conflict that 'would legitimize a scenario of war and military actions in the context of ICTs'.[159] This was a view shared by other States, notably China, which has consistently opposed the

---

[151] Declaration by Miguel Rodriguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, New York, 23 June 2017. There was also discussion of a so-called 'Digital Geneva Convention' which was originally proposed by Microsoft in 2017.

[152] Ibid.

[153] Cuba's statement was the only one publicly available, but there were suspicions that China and Russia also took this position.

[154] Rodriguez (n 151).

[155] Ibid.

[156] For example, references to the right to self-defence and the principles of countermeasures in relation to hostile acts in cyber-space were also found in a November 2015 declaration by the G20 (G20 Communique Antalya Summit, 15–16 November 2015) and in an April 2017 declaration by the G7 (G7 Declaration on Responsible States Behavior in Cyberspace, Lucca, 11 April 2017). In the academic literature see, e.g., *Tallinn Manual* (n 84) and Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017).

[157] Henriksen (n 143) 4, but with reference to James Lewis, 'Fighting the wrong enemy: aka the stalemate in cybersecurity', *The Cipher Brief* (2017) https://www.thecipherbrief.com/column/expert-view/fighting-the-wrong-enemy-aka-the-stalemate-in-cybersecurity.

[158] Michael Schmitt and Liis Vihul, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms' (30 June 2017) *Just Security*, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

[159] Rodriguez (n 151).

application of the 'military paradigm' to cyberattacks, as this risks aggravating 'the arms race and militarization in cyberspace'.[160] Therefore, in its view, 'the application of existing laws of armed conflict to cyberspace require[d] further scrutiny'.[161]

Unfortunately, the collapse of the GGE in 2017 left 'an unresolved international legal debate where the viewpoints seem[ed] to be diverging and solidifying rather than converging'.[162] Compounding the collapse of the GGE process was the fact that 2017 witnessed some of the most serious and disruptive cyber incidents, with the targeting and exploitation of governments, industries, and organizations across the world, 'from the international spread of WannaCry and Petya/NotPetya ransomware to dozens of large data breaches, including those that hit Equifax and Deloitte'.[163] Not only was one of the questions expected to be discussed by the 2016/17 Group possible 'ways and mechanisms to take the international debate beyond the current GGE format' but its collapse itself inevitably 'raise[d] the question of whether and how this legal debate, as well as the broader discussion of the GGE, [was] going to be continued'.[164] Indeed, some described the UN GGE process as 'dead'.[165] While some predicted that 'the June 2017 disappointment will probably only accelerate the creation of a more regionalized and fragmented regulation of cyberspace'[166] others spoke out in favour of continuing the GGE process.[167] However, other ideas were advocated in continuing the discussion, such as transferring it to an open-ended working group open to all,[168] the creation of a flexible and inclusive body within the OECD,[169] transferring it to an entirely new cyber committee of the UNGA,[170] moving the discussion into other committees of the UNGA, such as the sixth Committee, focusing entirely on legal questions,[171] or referring the matter – or at least the question regarding how international law applies to cyberspace – to the International Law Commission.[172] While '[t]he differences between the options may seem benign from the outside' they also

---

[160] Ma Xinmin,'Key issues and future development of international cyberspace law' (2016) 2 *China Quarterly of International Strategic Studies* 119, 128.

[161] Ibid.

[162] Elaine Korzak, 'UN GGE on cybersecurity: The end of an era?', *The Diplomat*, 31 July 2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

[163] Tim Maurer and Kathryn Taylor, 'Outlook on international cyber norms: Three avenues for future progress' (2 March 2018) *Just Security*, https://www.justsecurity.org/53329/outlook-international-cyber-norms-avenues-future-progress/.

[164] Korzak (n 162).

[165] Stefan Soesanto and Fosca D'Incau, 'The UN GGE is dead: Time to fall forward', *European Council on Foreign Relations* (15 August 2017) https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance.

[166] Henriksen (n 143) 8.

[167] Maurer and Taylor (n 163).

[168] Ibid.

[169] Theodore Christakis and Karine Bannelier, 'Reinventing multilateral cybersecurity negotiation after the failure of the UN GGE and Wannacry: The OECD solution' (28 February 2018) EJIL: *Talk!*, https://www.ejiltalk.org/reinventing-multilateral-cybersecurity-negotiation-after-the-failure-of-the-un-gge-and-wannacry-the-oecd-solution/.

[170] Maurer and Taylor (n 163).

[171] Ibid.

[172] François Delerue, 'The codification of the international law applicable to cyber operations: A matter for the ILC?' (3 July 2018) *ESIL Reflections*, https://esil-sedi.eu/wp-content/uploads/2018/06/ESIL-Reflection-Delerue.pdf.

had the potential to 'significantly shape the outcome of the diplomatic negotiations depending on who gets to sit at the table, what will be discussed, and whether discussions are bundled together or separated'.[173] The result, in the end, was what might be perceived as a 'splintering' of the process within the UN.[174]

(vi) A splintering of the process: The Sixth Group of Governmental Experts and the Open-Ended Working Group

Somewhat unexpectedly, in December 2018 two separate processes were established by the UN General Assembly to discuss the issue of cybersecurity and international law norms in relation to cyberspace during 2019-21. First, an open-ended working group (OEWG) was created,[175] an initiative proposed by a number of countries, including Russia.[176] While the GGE process had always been restricted to a number of 'experts', the OEWG represented the first time that all UN member States were invited to discuss developments in ICTs in the context of international security.[177] Indeed, the UNGA:

> *Decide*[ed] to convene … with a view to making the United Nations negotiation process on security in the use of information and communications technologies more democratic, inclusive and transparent, an open-ended working group acting on a consensus basis, to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States … and the ways for their implementation; if necessary, to introduce changes to them or elaborate additional rules of behaviour; to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations; and to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them and how international law applies to the use of information and communications technologies by States, as well as confidence-building measures and capacity-building and the concepts [referred to in the resolution].[178]

However, and to highlight the division in views among States as to how to proceed, the UNGA also opted to continue the debate within the framework of a GGE.[179] Indeed, the UNGA:

> *Request*[ed] the Secretary-General, with the assistance of a group of governmental experts, to be established in 2019 on the basis of equitable geographical distribution, proceeding from the assessments and recommendations contained in [the preceeding GGE reports], to continue to study, with a view to promoting common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States, confidence-building measures and

---

[173] Maurer and Taylor (n 163).

[174] Wyatt Hoffman, Duncan B. Hollis and Christian Ruhl, 'Cyber norms processes at a crossroads' (26 February 2020) *Lawfare*, https://www.lawfareblog.com/cyber-norms-processes-crossroads.

[175] UNGA Res 73/27, 5 December 2018, UN Doc. A/RES/73/27.

[176] It has been commented that '[b]y advocating for an OEWG, Russia tried to position itself as an advocate of democratic participation and inclusivity.' Alex Grigsby, 'The United Nations doubles its workload on cyber norms, and not everyone is pleased', *Council on Foreign Relations* (15 November 2018) https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

[177] Wider participation is something that had been advocated the previous year. See Maurer and Taylor (n 163).

[178] UN Doc A/RES/73/27 (n 175) para 5.

[179] UNGA Res 73/266 (22 December 2018) UN Doc A/RES/73/266.

> capacity-building, as well as how international law applies to the use of information and communications technologies by States, and to submit a report on the results of the study, including an annex containing national contributions of participating governmental experts on the subject of how international law applies to the use of information and communications technologies by States, to the General Assembly at its seventy-sixth session.[180]

This was supported by a number of countries, including Australia, France, Germany, the UK and the US. The resulting new GGE is composed of 25 expert members[181] and with the intention of submitting a final report to the UNGA in 2021 and will hold several meetings and two consultations with all UN Member States[182] as well as six regional consultations with the EU, the Organization for Security and Cooperation in Europe, the Organization of American States, the Association of Southeast Asian Nations Regional Forum, the African Union, and the League of Arab States.[183]

While the GGE was keen to reach out beyond the experts involved, the GGE and the OEWG nonetheless varied primarily on the scope of involvement of UN Member States. However, although the two groups have been described as 'mutually exclusive'[184] there is a clear overlap in their membership and the States involved, and the majority of States voted in favour of both groups with even many States that voted against the establishment of the OEWG ending up participating in its first meeting.[185]

The OEWG's mandate is slightly broader and also discusses existing and potential cyber threats as well as the establishment of a regular institutional dialogue and international concepts for securing global IT systems. However, both groups address cyber norms, confidence-building measures and the question of how international law applies to cyberspace. The proceedings of both groups are based on earlier substantive UN GGE reports, and therefore are proceeding on the basis that international law, and in particular the UN Charter, as well as the 'norms, rules and principles for the responsible behavior of States' included in the 2014/15 GGE report, are applicable to the ICT environment. It is notable, however, that the OEWG is also mandated to examine whether changes to them, or additional rules of behaviour, are necessary, something that the US and other States have consistently ruled out. A number of delegations confirmed this during the first meeting of the OEWG,[186] and others in working papers submitted to the chair of the group.[187] However, while there was clear agreement among States that these norms, rules and principles are essential to sustaining international peace and security in cyberspace, there was also agreement on the importance of developing a clearer understanding of them. The majority of State representatives confirmed that the 2014/2015 GGE report – the last successfully adopted report of the GGE process – should be the starting point for such further discussion.

---

[180] Ibid., para 3.

[181] The Member States participating in the 2019–2021 GGE are Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, Netherlands, Norway, Romania, Russian Federation, Singapore, South Africa, Switzerland, the UK, the US, and Uruguay.

[182] UN Doc A/RES/73/266 (n 179) para 5.

[183] Ibid., para 4.

[184] Grigsby (n 176).

[185] These States included Australia, France, the UK and the US.

[186] For example, China, Czech Republic, Egypt, Japan, Mexico, Russia, Singapore and Switzerland.

[187] These included, Australia, Canada, China, Iran, and the UK.

However, as with previous GGEs while there was agreement on the issue of the general applicability of international law and relevant norms and rules, there was palpable disagreement within the OEWG on more specific questions of applicability, and what should be the focus of the group going forward. For example, there was notable disagreement regarding the applicability of international humanitarian law. China, in particular, argued that in regard to the applicability of this branch of international law it is impossible to distinguish between civilian and military objects in cyberspace.[188] Other States shared this view about the focus of the group on IHL.[189]

Similarly, there was also concern, again, about focusing on issues related to the right of self-defence,[190] as well as the issue of sanctions and public attributions in responding to cyber attacks and other malicious activities.[191] Cuba expressed the view that doing so would make cyberspace a 'zone of conflict'.[192] While there was agreement that these were important issues there were concerns that focusing on them would lead to instability within the international community,[193] and that the focus of the group should instead be on the prevention of armed conflict, rather than on the applicability of these particular rules and principles.[194] However, a number of States, including the US, Australia and Norway opposed these views and were instead of the view that an agreement on the applicability of IHL and the right of self-defence would not lead to conflict and instability but rather would have the effect of emphasizing the importance of complying with these particular rules and norms as well as providing a 'plan B' should cyber conflict arose.[195]

Another issue where there was, again, disagreement was on the need for a new international cyber convention, with several States, including Russia, Syria and Iran, arguing for the need for a legally binding instrument.[196] While China was of the view that further study was needed as to which international laws were applicable in cyber space,[197] Syria suggested the establishment of a mechanism or body to examine the relevant international security issues regarding ICTs,[198] Iran suggested that any agreed upon instrument could incorporate legal rules and norms,[199] while Russia was clear that such an agreed upon instrument would not seek to change existing international law but would more explicitly adapt that law to the cyberspace context.[200] However, on this issue it was clear that a majority of representatives of the OEWG did not wish to see a new international instrument but rather to understand further existing legal rules and norms to the cyber environment – which were perceived as adequate as a guide for States in their activities in cyberspace – and the best way to implement them in the context of cyber

---

[188] Nele Achten, 'New U.N. debate on cybersecurity in the context of international security' (30 September 2019) *Lawfare*, https://www.lawfareblog.com/new-un-debate-cybersecurity-context-international-security.

[189] Ibid.

[190] Ibid.

[191] Ibid.

[192] Ibid.

[193] Ibid.

[194] Ibid.

[195] Ibid. See, in particular, Australia.

[196] Ibid.

[197] Ibid.

[198] Ibid.

[199] Ibid.

[200] Ibid.

security,[201] with some concerned that such an instrument would lower standards of protection as it would cover only certain issues.[202] The second substantive meeting of the OEWG took place at the beginning of February 2020 which witnessed States taking various positions on the applicability of international law to cyberspace, for example whether sovereignty is a principle or a rule of international law.[203] The final substantive session is due to take place in July 2020 with the Group reporting to the UNGA at its 75th session in September 2020.

Although the wisdom of having two parallel UN processes with the same mission might be questioned, in particular with providing the possibility of States to go 'forum shopping',[204] it might also be argued that 'at the very least they signal the extent to which U.N. member States share the view that international law plays a central role in shaping the behavior of States and non-State actors in cyberspace'.[205]

3. THE UNITED NATIONS SECURITY COUNCIL

The UN Security Council (UNSC) is the only body able to create binding international law.[206] The UNSC's resolutions to date have not generally been concerned with aspects of cyber-security. However, it has been active in the field of cyber-security, particularly terrorism-related aspects of it.

On 28 September 2001 the UNSC established the Counter-Terrorism Committee (CTC) through UNSC Resolution 1373 (2001) following the terrorist attacks of 11 September 2001.[207] The CTC has been involved in work to address the abuse of ICTs by terrorists and terrorist groups, in particular assessing States in implementing their counter-terror obligations under resolutions 1373 (2001), 1624 (2005), and 2178 (2014) in the context of ICT, and holding meetings on cyber-related terrorist issues. For example, in late 2015 it held a meeting on preventing terrorists from exploiting the internet to recruit terrorists and incite terrorist acts,[208] while in late 2016 it discussed preventing the exploitation of ICTs for terrorist purposes.[209] The Counter-Terrorism Committee Executive Directorate has also addressed the use of

---

[201] The initial meeting of the group also exposed potentially divergent views around human rights, social media content regulations and the development of offensive cyber capabilities.

[202] For example, Australia. See also statements of Canada, the Netherlands and the US.

[203] See Przemyslaw Roguski, 'The Importance of new statements on sovereignty in cyberspace by Austria, the Czech Republic and United States' (11 May 2020) *Just Security*, https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/.

[204] Grigsby (n 176).

[205] Michael N Schmitt, 'Norm-skepticism in cyberspace: Counter-factual and counterproductive' (28 February 2020) *Just Security*, https://www.justsecurity.org/68892/norm-skepticism-in-cyberspace-counter-factual-and-counterproductive/.

[206] UN Charter (1945) art 25.

[207] UNSC Res 1373 (28 September 2001) UN Doc S/RES/1373 para 6.

[208] Chair's summary, Special meeting of the Counter-Terrorism Committee with international and regional organizations on 'Preventing Terrorists from Exploiting the Internet and Social Media to Recruit Terrorists and Incite Terrorist Acts, While Respecting Human Rights and Fundamental Freedoms', New York, 17 December 2015, https://www.un.org/sc/ctc/wp-content/uploads/2016/09/Chair-summary-and-plan-of-action.pdf.

[209] Special meeting of the Security Council Counter-Terrorism Committee on preventing the exploitation of information and communication technologies (ICTs) for terrorist purposes, while respecting

ICT in terrorist activities, in particular through advising the CTC on its approach, organizing a number of events on countering terrorism through the use of ICTs, and launching a number of initiatives, such as that conducted with the Swiss Foundation ICT4Peace, which consists in working with the private sector and civil society to further understanding of industry responses to the use of new technology for terrorist purposes and identify good practices.

The Counter-Terrorism Implementation Task Force was also created by the UN Secretary-General in 2005 to ensure the coordination of the activities related to Resolution 1373 (2001).[210] The Task Force went on to establish various working groups, one of which was concerned with Countering the Use of the Internet for Terrorist Purposes. While this working group was established in response to the 9/11 attacks it later became linked to the broader cyber-security debate and today consists of various bodies, including Interpol, the Office of the High Commissioner for Human Rights and the United Nations Office on Drugs and Crime. The working group has four goals:[211]

- identify and bring together stakeholders and partners on the abuse of the Internet for terrorist purposes, including using the web for radicalization, recruitment, training, operational planning, fundraising and other means;
- explore ways in which terrorists use the Internet;
- quantify the threat that this poses and examine options for addressing it at national, regional and global levels; and
- examine what role the UN might play.

The group published its first report in February 2009 which analysed information provided by Member States and reflected the conclusions of a stakeholders' meeting held in November 2008.[212] Significantly, it concluded that at that moment there was no obvious terrorist threat in the area and that it was not obvious that it was a matter for action within the counter-terrorism remit of the UN. It did, however, outline ways suggested by Member States by which the UN could further contribute, including facilitating Member States sharing of best practices, building a database of research into use of the Internet for terrorist purposes, conducting more work on countering extremist ideologies, and creating international legal measures aimed at limiting the dissemination of terrorist content on the Internet.

In 2010 the working group began to build upon the work of the first report by addressing legal and technical challenges surrounding the efforts to counter the terrorist use of the Internet. The group held two meetings with various stakeholders and published a report in May 2011 which calls for a harmonization of national legislations by implementing regional instruments such as the Budapest Convention on Cybercrime or the Commonwealth Model Law on

---

human rights and fundamental freedoms, New York, 30 November-1 December 2016, https://www.un.org/sc/ctc/news/event/special-meeting-of-the-security-council-counter-terrorism-committee-on-preventing-the-exploitation-of-information-and-communication-technologies-ict-for-terrorist-purposes-while-respecting-human-ri/.

[210] This was endorsed by the UNGA Res 60/288 (20 September 2006) UN Doc A/RES/60/288 para 5.

[211] See Counter-terrorism Implementation Task Force, 'Working Group on Countering the Use of the Internet for Terrorist Purposes' http://www.un.org/en/terrorism/ctitf/wg_counteringinternet.shtml.

[212] UN Counter-terrorism Implementation Task Force, 'Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes' (February 2009) http://www.un.org/en/terrorism/ctitf/pdfs/wg6-internet_rev1.pdf.

Cybercrime as well as international instruments such as the Convention against Transnational Organized Crime.[213]

A third phase of the working group began in 2011 and focused on the use of the Internet to counter the appeal of terrorism, specifically by analysing the role of counter-narratives and effective messengers who can deliver these narratives. A report on this issue consisted of a summary of a conference held in Riyadh in January 2011 on 'The Use of the Internet to Counter the Appeal of Extremist Violence'.[214] Importantly, it was also agreed that '[g]iven the global nature of terrorist narratives and the need to counter them in the same space, there was a special role for the United Nations in facilitating discussion and action'.[215]

The Council has also had two Arria-formula meetings to discuss cybersecurity issues. Spain and Senegal jointly convened a meeting on 'Cybersecurity and International Peace and Security' in November 2016 which discussed how the use of ICTs may threaten international peace and security, in particular how countering cyber attacks can be particularly challenging due to, for example, the speed at which these attacks can be carried out and the difficulties regarding the attribution of them and holding the appropriate actors responsible. In addition, Council members were urged to explore ways to assess vulnerabilities and prevent cyber attacks and also to develop national strategies and policies, share best practices, commit to international cooperation, and form partnerships among governments, businesses, regional and sub-regional organizations, and civil society.[216] In March 2017 Ukraine convened a meeting of the Council on 'Hybrid Wars as a Threat to International Peace and Security' which included discussion of cyber threats, interference with political processes, and dissemination of propaganda. According to the concept note for the meeting hybrid warfare 'involves actions designed to fall below military response thresholds to deny or de-legitimate a military response from the target'.[217]

The activities of the UNSC in relation to cyber-security have also been guided by its membership. With Estonia's successful campaign for a seat in the Council during the 2020–21 term, and with its interest in issues of cyber-security, the topic will be given more of a focus in the discussions of the Council. Indeed, this has been a declared priority of Estonia, with the Estonian foreign minister Urmas Reinsalu (Isamaa) stating that;

> [a]s an elected member of the UNSC, one of Estonia's objectives is to raise awareness among members of the effects of cyber operations, and the validity of previously agreed international norms

---

[213] UN Counter-terrorism Implementation Task Force, 'Countering the Use of the Internet for Terrorist Purposes: Legal and Technical Aspects' (May 2011) http://www.un.org/en/terrorism/ctitf/pdfs/WG_Compendium-Legal_and_Technical_Aspects_2011.pdf.

[214] For the conference summary and follow-up/recommendations see UN Counter-terrorism Implementation Task Force, 'CTITF Working Group on Use of the Internet for Terrorist Purposes Riyadh Conference on Use of the Internet to Counter the Appeal of Extremist Violence' (January 2011) http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_riyadh_conference_summary_recommendations.pdf.

[215] Ibid.

[216] Security Council Report, 'In Hindsight: The Security Council and Cyber Threats' (23 December 2019) https://www.securitycouncilreport.org/monthly-forecast/2020-01/the-security-council-and-cyber-threats.php.

[217] Ibid.

> of behaviour. We are convinced that the UNSC must deal with new issues which threaten international peace and security but which are only gradually making their way on to the council agenda.[218]

It was significant that shortly after Estonia took its seat at the Council the issue of cybersecurity was prominently raised, with Estonia, the US and the UK condemning the October 2019 Russian cyberattacks against Georgia in a joint statement.[219]

4. THE ECONOMIC AND SOCIAL COUNCIL

The third (and final) intergovernmental body of the UN to deal with issues of cyber-security is the Economic and Social Council (ECOSOC) which is the principal body for coordination, policy review, policy dialogue and recommendations on economic, social and environmental issues. ECOSOC has held a general interest in issues of cyber-security and related issues. In 2010, it opened its session with a briefing title 'Cyber security: emerging threats and challenges' and the following year it held a special event on 'Cybersecurity and development'.[220] However, it is in two of its functional commissions – the Commission on Crime Prevention and Criminal Justice and the Commission on Narcotic Drugs – where most activity has occurred, particularly in connection with the criminal use of cyber-space.

(a) The Commission on Crime Prevention and Criminal Justice

The Commission on Crime Prevention and Criminal Justice (CCPCJ) was established by ECOSOC in 1992 and acts as the principal policymaking body of the UN in the field of crime prevention and criminal justice.[221] The first session of the Commission took place in 1992 with its work focusing on, as its name might suggest, crime and justice. In this respect, in 1998 the Commission requested the UNGA to include in the agenda of the Tenth Crime Congress a workshop on 'crimes related to the computer network'.[222] The following year, in 1999, the Commission also proposed a draft resolution for ECOSOC on the 'Work of the United Nations Crime Prevention and Criminal Justice Programme' requesting the Secretary-General to conduct a study on effective measures that could be taken at national and international levels to prevent and control computer-related crimes in light of the workshop at the Tenth Crime Congress and to report on his results at CCPCJ's tenth session.[223]

---

[218] 'Estonia raises cybersecurity issues at UN for first time', *ERR News* (6 March 2020) https://news.err.ee/1060642/estonia-raises-cybersecurity-issues-at-un-for-first-time.

[219] Permanent Mission of Estonia to the UN, 'Stakeout on cyber-attack against Georgia by Estonia, the United Kingdom and the United States' (5 March 2020) https://un.mfa.ee/press-stakeout-by-estonia-the-united-kingdom-and-the-united-states-on-cyber-attack-against-georgia/.

[220] See ECOSOC, '2010 ECOSOC General segment briefing on "Cyber security: emerging threats and challenges" – Background note' http://www.un.org/en/ecosoc/julyhls/pdf10/gs_briefing_background_note.pdf and ECOSOC, 'Special Event on Cybersecurity and Development – Informal summary' (9 December 2011) http://www.un.org/en/ecosoc/cybersecurity/summary.pdf.

[221] ECOSOC Res 1992/1 (6 February 1992). This was upon a request of the UNGA Res 46/152 (18 December 1991) UN Doc A/RES/46/152.

[222] ECOSOC E/1998/30-E/CN.15/1998/11.

[223] ECOSOC Res 1999/23 (28 July 1999). For the report of the UN Secretary General see ECOSOC E/CN.15/2001/4.

The ultimate result of the consideration given to such crimes at the Tenth Crime Congress in 2000 was the adoption by the UNGA of the Vienna Declaration on Crime and Justice, in which Member States:

> decide[d] to develop action-oriented policy recommendations on the prevention and control of computer-related crime, and we invite the Commission on Crime Prevention and Criminal Justice to undertake work in this regard, taking into account the ongoing work in other forums. We also commit ourselves to working towards enhancing our ability to prevent, investigate and prosecute high-technology and computer-related crime.[224]

At the CCPCJ's tenth session in 2001 a plan of action for implementing the Vienna Declaration was adopted including '[a]ction against high-technology and computer related crime' which recommended a series of national and international measures.[225] What was noticeable is that up until this point the focus was on computer crime as opposed to 'cyber' crime and security.[226] Indeed, it was only in the CCPCJ's 2002 report that the term 'cyber' was mentioned for the first time,[227] with a call for a UN convention on 'cybercrime' appearing in its 2004 report.[228] However, despite this activity it was only in 2010 that cyber-crime became a prominent theme in its annual reports, with some speakers again bringing up the possibility of a global convention against cyber-crime.[229] It was also notable the extent to which cyber-issues were prominent in the various issues discussed, including in the use of information technologies to exploit children, economic fraud and identity-related crime, and activities relating to combating cyber-crime including technical assistance and capacity-building. Subsequent reports have included discussion on, for example, cyber-crime in connection with the trafficking of cultural property,[230] and organized crime.[231]

Furthermore, ECOSOC and the UNGA requested the CCPCJ to establish, in line with paragraph 42 of the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, an open-ended intergovernmental expert group on cyber-crime.[232] This group was to conduct a comprehensive study of the problem of cyber-crime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cyber-crime.

---

[224] 'Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century, UNGA Res 55/59 (4 December 2000) para 18.

[225] ECOSOC E/2001/30/Rev.1-E/CN.15/2001/13/Rev.1

[226] Maurer (n 30) 37.

[227] ECOSOC E/2002/30-E/CN.15/2002/14.

[228] ECOSOC E/2004/30–E/CN.15/2004/16. This was by the representative of Thailand.

[229] ECOSOC E/2011/30-E/CN.15/2011/21.

[230] ECOSOC E/2014/30 E/CN.15/2014/20.

[231] Ibid.

[232] ECOSOC Res 2010/18 (22 July 2010); UNGA Res 65/230 (21 December 2010) UN Doc A/RES/65/230.

The first session of the group was held from 17 to 21 January 2011.[233] The UNGA noted with appreciation the work of the Expert Group and encouraged it to enhance its efforts to complete its work and to present the outcome of the study to the CCPCJ in due course.[234] The second session of the group was subsequently held from 25 to 28 February 2013.[235] The report includes discussion on issues such as legislation and frameworks, criminalization, law enforcement and investigations, electronic evidence and criminal justice, international cooperation and prevention. The third session of the group took place from 10 to 13 April 2017,[236] at which it considered, inter alia, the adoption of the summaries by the Rapporteur of deliberations at the first and second meetings of the Expert Group, the draft comprehensive study of the problem of cybercrime and comments thereto, and the way forward on the draft study, and exchanged information on national legislation, best practices, technical assistance and international cooperation. The fourth session of the group took place from 3 to 5 April 2018,[237] which focused on legislation and frameworks related to cybercrime, with different views expressed in relation to whether a new global instrument was required within the framework of the UN. The fifth session of the group took place from 27 to 29 March 2019,[238] which focused on law enforcement and investigations including electronic evidence and criminal justice. The sixth session of the group will take place from 6 to 8 April 2020 when it is due to discuss international cooperation and prevention, with a stocktaking meeting in 2021 to discuss the future of its work.

(b) The Commission on Narcotic Drugs

The Commission on Narcotic Drugs has focused on the use and abuse of the Internet only from a drug trafficking perspective in line with its functional mandate and did so as early as 1996.[239] In 2000 the Commission eventually adopted a resolution solely focused upon and titled 'Internet' which was brought to the attention of ECOSOC.[240] After the adoption of this resolution there was no further specific resolution on the Internet or cyber-issues, although repeated references were made to it as part of the Commission's discussions. However, in 2004, in

---

[233] The report on that meeting is contained in document UNODC, 'Report on the meeting of the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime held in Vienna from 17 to 21 January 2011' (31 March 2011) UN Doc UNODC/CCPCJ/EG.4/2011/3.

[234] UNGA A/RES/67/189 (27 March 2013).

[235] The report on that meeting is contained in document UNODC, 'Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 25 to 28 February 2013' (1 March 2013) UN Doc UNODC/CCPCJ/EG.4/2013/3.

[236] The report on that meeting is contained in document UNODC, 'Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 10 to 13 April 2017' (24 April 2017) UN Doc UNODC/CCPCJ/EG.4/2017/4.

[237] The report on that meeting is contained in document UNODC, 'Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 3 to 5 April 2018' (13 April 2018) UN Doc E/CN.15/2018/12.

[238] The report on that meeting is contained in document UNODC, 'Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 27 to 29 March 2019' (12 April 2019) UN Doc UNODC/CCPCJ/EG.4/2019/2.

[239] ECOSOC 'Commission on Narcotic Drugs: Report on the forty-second session' (1999) UN Doc E/1999/28/Rev.1.

[240] ECOSOC CND Res 43/8 (15 March 2000).

reference to the 2000 resolution, the Commission prepared a draft resolution for ECOSOC on the 'Sale of internationally controlled licit drugs to individuals via the Internet'.[241] In 2005, the Commission prepared a further resolution for ECOSOC titled 'Strengthening international cooperation in order to prevent the use of the Internet to commit drug-related crimes',[242] in 2007 it prepared a similar resolution on 'International cooperation in preventing the illegal distribution of internationally controlled licit substances via the Internet',[243] while in 2016 it prepared a further resolution on 'Promoting the protection of children and young people, with particular reference to the illicit sale and purchase of internationally or nationally controlled substances and of new psychotropic substances via the Internet'.[244]

5. SUBSIDIARY ORGANS AND SPECIALIZED AGENCIES

Aside from the intergovernmental bodies found within the UN Charter, there are several subsidiary organs and specialized agencies of the UN that work in the field of cyber-security. Although they are not expressly mentioned in the UN Charter it is here that they find their legal basis. Indeed, under Article 22 of the UN Charter '[t]he General Assembly may establish such subsidiary organs as it deems necessary for the performance of its functions' while Article 57 states that the 'various specialized agencies, established by intergovernmental agreement … shall be brought into relationship with the United Nations'. Of the many that exist, those key in the context of cyber-security are the International Telecommunications Unit, the United Nations Institute for Disarmament Research, and the United Nations Office on Drugs and Crime. Although an extensive analysis of their individual roles and functions is beyond the scope of this chapter, their key functions in connection with cyber-security will be briefly addressed.

(a) International Telecommunications Unit

The International Telecommunication Union (ITU) is the UN specialized agency for ICTs and has most responsibility for practical aspects of cyber-security. While it existed prior to the UN's founding in 1945 it subsequently joined the UN system as a specialized agency under Article 57 of the UN Charter. The ITU is not only a forum for discussion of cyber-security issues, and thus advances the broad agenda set by its Member States by focusing on specific initiatives, but it also plays a key role in setting technical standards.

The ITU Secretary-General launched the Global Cyber-Security Agenda in May 2007 which he described as being an 'international framework for cyber-security'.[245] A key part of this was the establishment of a high-level group of experts on cyber-security. The group

---

241 ECOSOC Res 2004/42 (21 July 2004).
242 ECOSOC CND Res 48/5 (2005).
243 ECOSOC CND Res 50/11 (2007).
244 ECOSOC CND Res 58/3 (2016).
245 Maurer (n 30) 30.

held three meetings between 2007 and 2008 before publishing its Global Strategic Report in 2008,[246] which focused on five areas:

- legal measures;
- technical and procedural measures;
- organizational measures;
- capacity-building; and
- international cooperation.

The recommendations of the group of experts to the ITU included:

- developing model legislation for Member States to adopt. The ITU has also developed a tool kit for cyber-crime legislation with sample language including explanatory comments which could form the basis for a harmonization of cyber-crime laws;
- the creation of a 'Cyber-security Readiness Index';
- a framework for national infrastructure protection; and
- a conceptualization of what a culture of cyber-security could be understood to mean.

The ITU Secretary-General has taken on a particularly visible role in the cyber-security agenda of the ITU. For example, at the 2010 World Telecom Development Conference in Hyderabad he proposed a 'no first attack vow' for cyberspace and that States 'should undertake not to harbour cyberterrorists and attackers in their country unpunished'[247] as well as drafting five principles of cyber-peace.[248] More recently in 2014, the ITU, along with the United Nations Children's Fund, and partners of the Child Online Protection Initiative, released updated Guidelines to strengthen online protection for children.[249] The ITU's initiatives in the context of Child Online Protection have 'been identified as an effort whose merit all states agree on and where trust can be built so that socialization effects could potentially produce positive spill over effects for the broader cyber-security agenda'.[250]

The current ITU cybersecurity programme builds on Objective 2 of the Buenos Aires Action Plan which was adopted at the 2017 World Telecommunication Development Conference,[251] and related resolutions. It offers Member States access to information and tools to increase cybersecurity at the national level 'in order to enhance security, build confidence and trust in the use of ICTs – making the digital realm more safe and secure for everyone'.[252]

---

[246] See 'Global Cybersecurity Agenda (GCA)' (ITU) http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf.

[247] Henning Wegener, 'Cyber peace', in International Telecommunication Union and World Federation of Scientists, *The Quest for Cyber Peace* (ITU 2011) 81 http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf.

[248] Ibid., 78.

[249] See 'COP Guidelines' (ITU) http://www.itu.int/en/cop/Pages/guidelines.aspx.

[250] Maurer (n 30) 30.

[251] See Final Report, World Telecommunication Development Conference, Buenos Aires (9-20 October 2017) https://www.itu.int/en/ITU-D/Conferences/WTDC/WTDC17/Documents/WTDC17_final_report_en.pdf.

[252] See https://www.itu.int/en/ITU-D/Cybersecurity/Pages/about-cybersecurity.aspx.

(b) United Nations Institute for Disarmament Research

The United Nations Institute for Disarmament Research (UNIDR) is a voluntarily funded autonomous institute within the UN and generates ideas and promotes action on disarmament and security. It was one of the first UN bureaucracies to become involved in the issue of cyber-security and today its 'cyber work aims to carry out policy-focused capacity-building at the national, regional and multilateral level, as well as relevant research and analysis'.[253]

It has hosted two conferences relating to the discussions in the UNGA's First Committee. In 1999, the United Nations Department for Disarmament Affairs funded a two-day discussion meeting on 'Developments in the field of information and telecommunications in the context of international security'.[254] This conference was titled the same as the resolution introduced by Russia a year earlier and highlighted the different primary concerns that States had at that time. In 2008 Russia then funded a conference on 'Information and Communication Technologies and International Security' with the objective being '[t]o examine the existing and potential threats originating from the hostile use of information and communication technologies, discuss the unique challenges posed by ICTs to international security and possible responses'.[255]

Today, as well as acting as a consultant to the GGEs and providing the Cyber Policy Portal, which is an online reference tool that maps the cybersecurity and cybersecurity-related policy landscape, it also hosts annual cyber-stability conferences. The conference in June 2019 provided an opportunity for experts from the UN and regional international organizations, private sector, technical community and academia to examine the current state of discussions on global cybersecurity policy, including UN GGE and OEWG on cybersecurity, norms and efforts to tackle threats emanating from the use of ICTs and ways of strengthening them.

(c) United Nations Office on Drugs and Crime

Although cyber-security is not formally within the domain of the UN Office on Drugs and Crime (UNODC), the Third Committee of the UNGA first requested for UNODC to become involved in technical assistance specifically relating to 'cyber crime' in 2008.[256] The UNODC draws upon its specialized expertise on criminal justice systems response to provide technical assistance in capacity building, prevention and awareness raising, international cooperation, and data collection, research and analysis on cybercrime.

Member States officially requested UNODC to work on the use of the Internet for terrorist purposes for the first time at the 20th session of the Commission on Crime Prevention and Criminal Justice in April 2011 after it was first mentioned at the 19th session the year before. UNODC's Terrorism Prevention Unit contributed to a CTITF publication in 2012 for law enforcement investigators and criminal justice officers in connection with cases involving

---

[253] See 'Cyber' (United Nations Institute for Disarmament Research) http://www.unidir.org/est-cyber.

[254] Maurer (n 30) 28.

[255] Ibid.

[256] UNGA Res 63/195 (18 December 2008) UN Doc A/RES/63/195.

'[t]he use of the internet for terrorist purposes'.[257] It also has adopted a leading role in the Global Programme on Cybercrime which, as described above,[258] was initiated by the CCPCJ and which aims to assist Member States in strengthening existing national and international legal responses to cybercrime. The Programme is based within the UNODC Organized Crime Branch which is a part of the Division for Treaty Affairs. As a part of the Global Programme on Cybercrime, the Cybercrime Repository provides a data repository of cybercrime laws and lessons learned for the purposes of facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance.

6. CONCLUSION

Finnemore and Sikkink have perceptively observed that '[n]orms do not appear out of thin air; they are actively built by agents having strong notions about appropriate or desirable behaviour in their community'.[259] This chapter has only been able to offer a somewhat limited account of the activities of the UN and its Member States in the context of cyber-security. Yet, it is clear that while there remain divisions within the UN, and in particular within the GGE and OEWG, regarding the focus of any emerging regulatory framework and the underlying approach to govern cyberspace, there has been a discernable shift in the will among States to take action to regulate activity within cyberspace in some form. Achievements in the context of norm development in this area can be seen in the number of UNGA resolutions adopted in various committees, the increasing number of sponsors of these resolutions, the progressive work of the GGEs and the OEWG, and the work on the issue of cyber-security taking place across a range of organs, agencies and bodies. Indeed, we have witnessed a distinct shift in activity, and perhaps momentum towards something substantial and meaningful being achieved within and by the UN. The general applicability of international law, the need for practical cooperation between not just States but also between States and other stakeholders, the need to develop common understandings of acceptable State behaviour, and the need for confidence-building, transparency and capacity-building measures have become themes cemented most visibly within the discourse of the GGEs but also discernable in the work of the other UN organs. As commented by Michael Schmitt, '[w]hile it is no doubt true that further clarity is needed, and that compliance and enforcement must be improved, the trend is very positive overall. In this regard, U.N. efforts are particularly noteworthy'.[260]

Yet, and in particular given the recent splintering of the process within the UN, it would be short-sighted to think that a regulatory framework can emerge solely within the forum of the UN. Indeed, the UN itself has continuously noted the valuable efforts that have been made by international organizations and regional entities in this area, such as the African Union, ASEAN, the Council of Europe, ECOWAS, the EU, and the Shanghai Cooperation Organization, to name a few. Further, States have begun to act bilaterally in seeking to cooper-

---

[257] UNODC, 'The use of the internet for terrorist purposes' (UN, 2012) http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

[258] See section 4(a) above on the CCPCJ.

[259] Martha Finnemore and Kathryn Sikkink, 'International norm dynamics and political change' (1998) 52 *Intl Organization* 887, 894–6.

[260] Schmitt (n 205).

ate, come to common understandings, and build confidence and transparency between them in their operations in cyberspace. A good example of this is the working group on cyber-security established between the US and China in 2013,[261] with the subsequent 2015 agreement between the two States regarding the cyber-enabled theft of intellectual property.[262] This in many respects remains one of the most effective commitments thus far with multiple reports that it has contributed to a slowdown in malicious activity between the two States,[263] and the Trump administration has stated that its approach to cyber norms will shift further from multilateral to bilateral engagements.[264]

As such, it is not strictly accurate to claim that '[t]he conflicting currents of state views as evidenced in the First Committee debates are unlikely to be resolved via the GGE process', as, and as set out above, the GGEs *have* adopted positions accommodating – albeit in a somewhat equivocal fashion – of the two main streams of views. However, it is still nonetheless the case that while the reports of the GGEs are of constructive use States will ultimately also 'have to look to other multilateral, regional and bilateral forums to see what might be feasible in terms of confidence building measures and agreed norms of behaviour'.[265]

---

[261] 'US and China to set up cyber security working group', *BBC News* (13 April 2013) http://www.bbc.co.uk/news/world-asia-china-22137950.

[262] Fact Sheet, President Xi Jinping's State Visit to the United States (25 September 2015) https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[263] David E. Sanger, 'Chinese Curb Cyberattacks on U.S. Interests, Report Finds', *New York Times* (20 June 2016) https://www.nytimes.com/2016/06/21/us/politics/china-us-cyber-spying.html.

[264] The White House, Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017, 26 June 2017, https://www.whitehouse.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017/.

[265] 'UN GGE – Cyber Security takes the UN Floor', ICT For Peace Foundation (17 November 2013) https://ict4peace.org/activities/cyber-security-takes-the-un-floor/.

Index