Routledge Handbook of International Cybersecurity

Edited by Eneken Tikk and Mika Kerttunen

ROUTLEDGE HANDBOOK OF INTERNATIONAL CYBERSECURITY

The *Routledge Handbook of International Cybersecurity* examines the development and use of information and communication technologies (ICTs) from the perspective of international peace and security.

Acknowledging that the very notion of peace and security has become more complex, the volume seeks to determine which questions of cybersecurity are indeed of relevance for international peace and security and which, while requiring international attention, are simply issues of contemporary governance or development. The Handbook offers a variety of thematic, regional and disciplinary perspectives on the question of international cybersecurity, and the chapters contextualize cybersecurity in the broader contestation over the world order, international law, conflict, human rights, governance and development.

The volume is split into four thematic sections:

- Concepts and frameworks;
- Challenges to secure and peaceful cyberspace;
- National and regional perspectives on cybersecurity;
- Global approaches to cybersecurity.

This book will be of much interest to students of cybersecurity, computer science, sociology, international law, defence studies and International Relations in general.

Eneken Tikk is Executive Producer of the Cyber Policy Institute, Estonia, and lead of the International Law project at CPI and the Erik Castrén Institute, University of Helsinki, Finland.

Mika Kerttunen is Director of Strategy at the Cyber Policy Institute, and Senior Research Scientist at the Tallinn University of Technology, Estonia.

Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

ROUTLEDGE HANDBOOK OF INTERNATIONAL CYBERSECURITY

Edited by
Eneken Tikk and Mika Kerttunen

First published 2020
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN
and by Routledge
52 Vanderbilt Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

© 2020 selection and editorial matter, Eneken Tikk and Mika Kerttunen;
individual chapters, the contributors

The right of Eneken Tikk and Mika Kerttunen to be identified as the
authors of the editorial material, and of the authors for their individual
chapters, has been asserted in accordance with sections 77 and 78 of the
Copyright, Designs and Patents Act 1988.

With the exception of Chapter 30, no part of this book may be reprinted
or reproduced or utilised in any form or by any electronic, mechanical, or
other means, now known or hereafter invented, including photocopying
and recording, or in any information storage or retrieval system, without
permission in writing from the publishers.

Chapter 30 of this book are available for free in PDF format as Open
Access from the individual product page at www.routledge.com. These
have been made available under a Creative Commons Attribution-Non
Commercial-No Derivatives 4.0 license.

Trademark notice: Product or corporate names may be trademarks
or registered trademarks, and are used only for identification and
explanation without intent to infringe.

British Library Cataloguing-in-Publication Data

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

Library of Congress Cataloging-in-Publication Data

A catalog record has been requested for this book

ISBN: 978-1-138-48901-1 (hbk)

ISBN: 978-1-351-03890-4 (ebk)

Typeset in Bembo
by codeMantra

CONTENTS

<i>List of illustrations</i>	<i>ix</i>
<i>Acknowledgements</i>	<i>x</i>
<i>Foreword</i>	<i>xi</i>
Joseph S. Nye, Jr.	
<i>List of contributors</i>	<i>xiv</i>
 Introduction	 1
<i>Mika Kerttunen and Eneken Tikk</i>	
 PART I	
Concepts and frameworks	9
 1 Cybersecurity between hypersecuritization and technological routine	 11
<i>Myriam Dunn Cavelty</i>	
 2 Correlates of state-sponsored cyber conflict	 22
<i>George E. Mitchell and Allison Pytlak</i>	
 3 Cybered conflict, hybrid war, and informatization wars	 36
<i>Chris C. Demchak</i>	
 4 The politics of stability: cement and change in cyber affairs	 52
<i>Mika Kerttunen and Eneken Tikk</i>	
 5 In search of human rights in multilateral cybersecurity dialogues	 65
<i>Allison Pytlak</i>	

6	International governance of/in cyberspace <i>Tang Lan (translated by Nigel Inkster)</i>	79
7	The becoming of cyber-military capabilities <i>Mirva Salminen and Mika Kerttunen</i>	94
PART II		
Challenges to secure and peaceful cyberspace		109
8	Cyber vulnerability <i>Brian Martin</i>	111
9	Ensuring the security and availability of critical infrastructure in a changing cyber-threat environment: living dangerously <i>Vytautas Butrimas</i>	122
10	Steps to an ecology of cyberspace as a contested domain <i>Martin C. Libicki</i>	134
11	Cybercrime: setting international standards <i>Tatiana Tropina</i>	148
12	Cyberterrorism: a Schrödinger's cat <i>Mika Kerttunen</i>	161
13	Information operations <i>Jouni Flyktman, Aki-Mauri Huhtinen and Lars Koreman</i>	174
14	National cyber commands <i>Piret Pernik</i>	186
PART III		
National and regional perspectives on cybersecurity		199
15	Cyber capacity-building and international security <i>Souhila Amazouz</i>	201
16	Challenges in building regional capacities in cybersecurity: a regional organizational reflection <i>Belisario Contreras and Kerry-Ann Barrett</i>	214
17	Singapore, ASEAN, and international cybersecurity <i>Benjamin Ang</i>	218

18	Sub-regional views on international cybersecurity: CLMV countries <i>Lim Ratha and Sok Kuvath</i>	227
19	Regional cybersecurity approaches in Africa and Latin America <i>Lucy Purdon and Francisco Vera</i>	234
20	A regional view on international cybersecurity: the scope, problem, and remedies as seen in West Africa <i>Folake Olagunju Oyelola</i>	247
21	Risk, resilience, and retaliation: American perspectives on international cybersecurity <i>James A. Lewis</i>	252
22	International information security: problems and ways of solving them <i>Andrei V. Krutskikh and Anatoli A. Streltsov (translated by Eneken Tik)</i>	260
23	People's Republic of China: seven cybersecurity considerations <i>Zhang Li</i>	269
PART IV		
	Global approaches to cybersecurity	275
24	Cyber diplomacy: an Australian perspective <i>Tobias Feakin and Johanna Weaver</i>	277
25	Confidence-building measures in cyberspace: new applications for an old concept <i>Paul Meyer</i>	286
26	Export controls: the Wassenaar experience and its lessons for international regulation of cyber tools <i>Elaine Korzak</i>	297
27	Global cybersecurity and the private sector <i>Anne-Marie Buzatu</i>	312
28	Putting the technical community back into cyber (policy) <i>Pablo Hinojosa, Klée Aiken and Louise Marie Hurel</i>	326
29	Economic cybersecurity law: a short primer <i>Kathleen Claussen</i>	341

Contents

30	The role of the UN Security Council in cybersecurity: international peace and security in the digital age <i>Eneken Tikk and Niels Nagelhus Schia</i>	354
31	International law and cyber conflict <i>Gary D. Brown</i>	366
32	Exploring the general principles of international law in the cybersecurity context <i>Nohyoung Park and Myung-Hyun Chung</i>	379
33	What do we talk about when we talk about international cybersecurity <i>Eneken Tikk</i>	389
	<i>Index</i>	397

ILLUSTRATIONS

Figures

2.1	Probability of cyber conflict initiation as a function of state B's GDP	30
2.2	Probability of cyber conflict initiation as a function of state A's voice and accountability score	31

Tables

2.1	Hypotheses and results	28
2.2	Population averaged models for cyber conflict initiation	29
2.3	Fixed effects models for cyber conflict initiation	31
8.1	Communication vulnerabilities for a government with repressive elements	115
8.2	Communication vulnerabilities for an opposition movement to a repressive government	115
30.1	Summary of the UN GGE 2010, 2013 and 2015 reports argumentation of the threats	358

ACKNOWLEDGEMENTS

This Handbook would not have seen the light of day without the uncompromised dedication of our contributors. These authors, ranging from a septuagenarian to a millennial, from formally retired to recently employed, from Classical Realists to Social Constructivists to reflective Idealists, from the so-called first world to those from the so-called third world, are paving ways through a much debated but less researched terrain of international cybersecurity. They have balanced through professional and personal commitments, even some (fortunately temporal) physical handicaps. Viewing the list of contributors makes us proud, humble and privileged: what a group of experts!

However, without the compassion of numerous colleagues, friends and family members, the authors and the editors could not have prevailed. On the behalf of all the contributors, thank you for your invaluable support.

We, the editors, want to thank Mr. Andrew Humphrys and Ms. Bethany Lund-Yates at Taylor and Francis for their kind and professional support. Also, the reviewers of our original proposal, who both saw value in a handbook of international cybersecurity and forced us to rethink our initial approach, deserve our warm thanks.

We hope that, because of our contributor's wisdom and despite the editors' shortcomings, the *Routledge Handbook of International Cybersecurity* manages to provide useful guidance to students, scholars and statesmen alike.

Tartu and Jyväskylä
Eneken Tikk Mika Kerttunen

FOREWORD

Like many important terms used in policy and social science, cybersecurity is a contested concept. As Mika Kerttunen and Eneken Tikk point out in the Introduction, it is not only a new term but it covers a wide range of problems. And that makes the rich variety of articles in this handbook all the more valuable.

Security was not a major concern among the small community of researchers and programmers who developed the Internet in the 1970s and 1980s. Even in 1996, only 36m people (about 1 per cent) of the world population used the Internet. Disruptive malware and denial-of-service attacks were more a nasty nuisance for a relatively restricted community rather than a major international security problem. However, within two decades, 3.7bn people, or nearly half the world population, were connected to the Internet and international cybersecurity had become a major international issue.

As the number of users escalated after the late 1990s, the Internet became a vital substrate for economic, social and political interactions and this new interdependence created great economic and social opportunity. However, as Robert Keohane and I pointed out in 1977, well before the burgeoning of the Internet, interdependence also creates vulnerability and insecurity. Power and interdependence are closely intertwined. Contrary to the utopian libertarian expectations of its earlier days, this century's growth of the Internet in an anarchic world of states and non-state actors was bound to create new issues of international cybersecurity. With big data, machine learning and the 'Internet of Things', many experts anticipate that the number of Internet connections will continue to grow exponentially. The potential attack surface will expand dramatically and include everything from industrial control systems to heart pacemakers to self-driving cars to social media and electoral systems. The cyber domain will provide opportunities for both private and interstate conflict, or what Chris Demchak calls in her chapter 'cybered conflict'.

Many observers have called for laws and norms to manage the new international insecurity created by information technology and cyberspace. For example, in 2018 UN Secretary-General António Guterres called for 'global rules to minimize the impact of electronic warfare on civilians as massive cyberattacks look likely to become the first salvoes in future wars'. He appointed a High Level Panel on the subject which issued its report on *The Age of Digital Interdependence* in June 2019. Many other commissions and organizations, public and private, have issued reports on cybersecurity.

There are a variety of scenarios regarding cyberconflict discussed in the essays below, but despite pleas from leaders over the years, the development of norms to limit conflict faces a number of difficult hurdles in the cyber domain. Just to name a few: non-state actors play a major role, some malign and some benign. The Internet is a transnational network of networks, most of which are privately owned, and companies with vast decision spans affect many norms. Unlike most military arenas, the cyber domain has multiple stakeholders in addition to governments. Cyber tools can be dual use, fast, cheap and often deniable. Depending upon time and degree of certitude, verification and attribution can be difficult. Here too private entities play a role and barriers to entry are falling. Major states differ in their objectives, with Russia and China stressing the importance of sovereign control and many democracies pressing for a more open multi-stakeholder Internet. While the Internet is transnational, the infrastructure (and people) on which it rests fall within the competing jurisdictions of sovereign states.

Cyber is not the first disruptive technology that the international system has encountered since World War II. The split atom was enormously disruptive. States and societies will have to learn to cooperate on cybersecurity in an analogy to how they learned to cooperate in regard to nuclear weapons. While cyber and nuclear technologies are vastly different in their characteristics and effects, at a meta level, we can study the processes of how societies and states learn. One daunting lesson is how long learning and agreement takes. It took about two decades to reach the first cooperative agreements to limit conflict in the nuclear era. If one dates the international cyber security problem from when the web was commercialized (along the lines discussed above), intergovernmental cooperation in cyber is now at about the two-decade mark. Cyber time moves quickly, but human habits, norms and state practices change more slowly.

It was not until after the frightening Cuban Missile Crisis in 1962 that a first arms control agreement, the Limited Test Ban Treaty, was signed in 1963. The Non-Proliferation Treaty followed in 1968 and the bilateral Strategic Arms Limitation Treaty in 1972. In 1998, Russia first proposed a UN treaty to ban electronic and information weapons (including for propaganda purposes). With China and other members of the Shanghai Cooperation Organization, it has continued to push for a broad UN-based treaty. The USA resisted what it saw as an effort to limit free expression on the Internet, and continues to view a broad treaty as unverifiable and thus deceptive. Instead, the USA and 13 other states agreed to a Russian proposal that the UN Secretary-General should appoint a group of governmental experts (UNGGE), which first met in 2004. Five GGEs have met within the framework of the UN First Committee Resolution on 'Developments in the Field of Information and Telecommunications in the Context of International Security'. This cumbersome title incorporated both the Russian focus on 'information warfare' and the US focus on cyber operations.

Initially the GGE process had meagre results, but gradually its members agreed to support a wider process of defining both norms of state behaviour as well as embark on concrete discussions on confidence-building measures. The GGE issued reports in 2010, 2013 and 2015 that helped to set the negotiating agenda for cyber security. In July 2015, it proposed a set of norms that was later endorsed by the Group of Twenty (G20). The success of this group was above the ordinary, but it failed to agree on a new report in 2017. As the issue grew in salience and relations among the major powers worsened international cybersecurity became more politicized. The number of members of the GGE increased from the original 15 to 20 to 25, but many nations complained that they did not have a voice. A dual process was established in the UN system with a new GGE as well as an Open-Ended Working Group which all members could join, but the outcome remains uncertain.

Foreword

One thing is sure, the problem of international cybersecurity is here to stay and is likely to grow in importance. That makes the existence of this volume with its diversity of topics and excellent authors all the more important.

*Joseph S. Nye, Jr.
Kennedy School of Government
Harvard University*

CONTRIBUTORS

Klée Aiken is a Chicagoan lost in the Asia-Pacific. Klée is an ex-think tanker now exploring the world of Internet governance, cyber policy, and capacity building as APNIC Senior Advisor and Advisory Board member for the Global Forum on Cyber Expertise.

Souhila Amazouz is Senior Policy Officer at the African Union Commission (AUC) Information Society division. Ms. Amazouz works on the development of the Information Society in Africa, coordination of regional and continental initiatives, harmonizing the legislations and policy guidance on critical and emerging global issues such as cybersecurity, Internet Governance, broadband strategies and spectrum management. Previously she worked more than 10 years with the Algerian Broadcasting Corporation as a Chief Engineer specialized in spectrum management and network planning.

Benjamin Ang leads the Cyber and Homeland Defence Programme in the Centre of Excellence for National Security at S. Rajaratnam School of International Studies. He has a multi-faceted career including time as a litigation lawyer, IT Director and General Manager of a major Singapore law firm, corporate lawyer specialising in technology law and intellectual property issues, in house legal counsel in an international software company, Director-Asia in a regional technology consulting firm, in-house legal counsel in a trans-media company, and senior law lecturer at a local Polytechnic, specialising in data privacy, digital forensics, and computer misuse and cybersecurity.

Kerry-Ann Barrett is the Cyber Security Policy Specialist at the Cyber Security Program, Inter-American Committee against Terrorism (CICTE), Secretariat for Multidimensional Security at the Organization of American States. Most recently, she has led and provided technical support for the development of the national cyber security strategies for the Barbados, Belize, Costa Rica, Dominica, Mexico, Jamaica, Suriname, Dominican Republic and has helped Colombia and Peru in developing their national cybersecurity frameworks.

Gary Brown is Professor of Cyber Law, College of Information and Cyberspace, National Defense University, Washington, DC. He participated in the drafting process for the first

Tallinn Manual (Cambridge, 2013) and was a member of the group of experts that drafted *Tallinn Manual 2.0* (Cambridge, 2017).

Vytautas Butrimas with over 29 years of experience in IT security and defense policy is part of Lithuania's national contribution (from the Ministry of National Defence] to the NATO Energy Security Centre of Excellence where he serves as a Cybersecurity Subject Matter Expert.

Anne-Marie Buzatu is co-founder and director of Security and Human Empowerment Solutions based in Geneva, Switzerland. Previous publications include *The Emergence of the International Code of Conduct for Private Security Service Providers* (Routledge April 2016), *Towards an International Code of Conduct for Private Security Providers: A View from Inside a Multi-Stakeholder Process*, DCAF SSR Paper 12, November 2015, and *Multistakeholder Approaches to Governance: Challenges and Opportunities*, DCAF Horizon 2015 Working Paper Series, 2016.

Myung-Hyun Chung is Research Professor at the Korea University School of Law Cyber Law Centre. Her research interests cover international law, international economic law and cyber war and terrorism.

Kathleen Claussen is Associate Professor at the University of Miami School of Law. She has published on international economic law and security topics in journals such as the Yale Law Journal, Stanford Law Review, and American Journal of International Law. She is a graduate of the Yale Law School.

Belisario Contreras currently leads and coordinates the Cybersecurity capacity building efforts at the Organization of American States (OAS). He is member of the Global Cybersecurity Board at the World Economic Forum (WEF) and is also an Oxford University Fellow. In this capacity he has been a frequent speaker at international and regional cyberspace events, bringing attention to the specific impact these issues have on the LAC region.

Chris C. Demchak is US Naval War College's Hopper Chair of Cyber Security. With engineering, economics, complexity, comparative organizations background, her work is systemic: insecure cyberspace 'substrate', cybered conflict, Cyber Westphalia, socio-technical-economic systems, and democratic 'Cyber Operational Resilience Alliance'. Recent works: *Designing Resilience*; *Wars of Disruption and Resilience*; and drafts: *Cyber Westphalia* and *Cyber Commands*.

Myriam Dunn Cavelty is Senior Lecturer and deputy for research and teaching at the Center for Security Studies (CSS) at ETH Zurich. Myriam is the author of *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (Routledge Hardback 2008, Paperback in 2009).

Tobias Feakin is Australia's inaugural Ambassador for Cyber Affairs. Dr Tobias Feakin is Australia's inaugural Ambassador for Cyber Affairs. He was the Director of National Security Programs at the Australian Strategic Policy Institute from 2012 to 2016 establishing the Institute's International Cyber Policy Centre. Dr Feakin has also held research and advisory positions, including with the Royal United Services Institute for Defence and Security Studies, the Oxford University Global Cyber Security Capacity Centre, the

Global Commission on Internet Governance and the Global Commission on the Stability of Cyberspace.

Jouni Flyktman (Major, G.S.) serves as a program manager in the Defence Command Finland. He has degrees in engineering physics, economics and military science. His experience includes positions in cyber defence and electronic warfare. He has studied information warfare in the Finnish National Defence University.

Pablo Hinojosa is an expert in Internet governance. He is currently Strategic Engagement Director at APNIC. Before joining APNIC, he was Regional Relations Manager at ICANN. Before ICANN, he was Director for Multilateral Affairs in the Mexican Telecommunications Regulator.

Aki-Mauri Huhtinen (LTC (GS)) is a military professor at the Finnish National Defence University in the Department of Leadership and Military Pedagogy. His areas of expertise are military leadership, command and control, information warfare, the philosophy of science in military organizational research and the philosophy of war.

Louise Marie Hurel is pursuing her PhD in Data, Networks, and Society at the London School of Economics working on technical security expertise and cybersecurity governance. Louise Marie also heads research and project development at Igarapé Institute's Cybersecurity and Digital Liberties Programme.

Mika Kerttunen is co-founder of the Cyber Policy Institute, and Senior Research Scientist at the Tallinn University of Technology Centre for Digital Forensics and Cyber Defence. His professional work and research interests cover e.g. cyber-diplomacy (NUPI, 2018), national cybersecurity strategies (EUISS, 2019). And capacity-building. He served as advisor to the Finnish UN GGE expert in 2016–2017.

Lars Koreman (LtCol, German Bundeswehr) is a defense communication practitioner, researcher and lecturer on Strategic Communications. Currently he is a student fellow at the George C. Marshall European Center for Security Studies. He holds a university degree in business administration and economics.

Elaine Korzak is Visiting Assistant Professor of Cybersecurity at the Middlebury Institute of International Studies at Monterey (MIIS) where she leads the Cyber Initiative. She was previously a National Fellow at the Hoover Institution and a cybersecurity fellow at CISAC. Her professional experience includes various governmental and non-governmental institutions where she has worked on various disarmament and international security issues. These include NATO's Cyber Defence Section as well as the European Commission's Directorate-General on Information Society and Media.

Andrei V. Krutskikh is Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security, Doctor of Historical Sciences and Professor at Moscow Lomonosov University. Ambassador Plenipotentiary Krutskikh has been Russian expert in all six UN Groups of Governmental Experts on Information Security.

James A. Lewis is a Senior Vice President at the Center for Strategic and International Studies (CSIS). Before joining CSIS, he worked for the U.S. government. He was the advisor for the 2010, 2013 and 2015 UN Group of Governmental Experts on Information Security and has authored many publications on cybersecurity.

Martin C. Libicki holds the Keyser Chair of cybersecurity studies at the U.S. Naval Academy. He is the author of a 2016 textbook on cyberwar, *Cyberspace in Peace and War, Conquest in Cyberspace: National Security and Information Warfare*, and *Information Technology Standards: Quest for the Common Byte*. He is also the author of numerous RAND monographs, notably *Defender's Dilemma*, *Brandishing Cyberattack Capabilities*, *Crisis and Escalation in Cyberspace*, *Global Demographic Change and its Implications for Military Power*, and *Cyberdeterrence and Cyberwar*.

Ratha Lim has 14 years of experience working in different NGOs, IOs and law firms in Phnom Penh. She completed her Master in Practices of International Solidarity from Nice Sophia-Antipolis University in France and International Business Law and Corporate Counsel from Royal University of Law and Economics in Cambodia.

Brian Martin is emeritus professor of social sciences at the University of Wollongong, Australia. He is the author of 19 books and hundreds of articles on nonviolent action, whistleblowing, scientific controversies and other topics.

Paul Meyer is an Adjunct Professor of International Studies at Simon Fraser University in Vancouver and a Senior Advisor with ICT4Peace. A former career Canadian diplomat specializing in international security policy, he has written extensively on issues of cyber security diplomacy and arms control.

George E. Mitchell is an associate professor at the Marxe School of Public and International Affairs at Baruch College of the City University of New York. His published research has examined topics in NGO and non-profit studies, public administration, international relations, and cyber conflict.

Joseph S. Nye Jr., University Distinguished Service Professor, Emeritus and former Dean of the Harvard's Kennedy School of Government. He has served as Assistant Secretary of Defense for International Security Affairs, Chair of the National Intelligence Council, and Deputy Under Secretary of State for Security Assistance, Science and Technology. His most recent books include *The Power to Lead*; *The Future of Power*; *Presidential Leadership and the Creation of the American Era*; and *Is the American Century Over*. He is a fellow of the American Academy of Arts and Sciences, the British Academy, and the American Academy of Diplomacy.

Folake Olagunju Oyelola is the Internet and Cybersecurity Programme Officer at the ECOWAS Commission. She is currently working on implementing the cybersecurity agenda to facilitate initiatives that will assist the ECOWAS region protect their cyberspace, critical information infrastructure and build confidence in the use of ICTs.

Nohyoung Park is the Dean of School of Law, and the Director of the Cyber Law Centre at Korea University. He graduated from the College of Law, Korea University (LL.B., 1981),

the Graduate School, Korea University (LL.M., 1983), Harvard Law School (LL.M., 1985), and the University of Cambridge (Ph.D. in International Law, 1990). His main research interests cover international economic law, negotiation and mediation, and cyber security, cyber war and privacy and data protection.

Piret Pernik is cyber security researcher at the Internal Security Institute of the Estonian Academy of Security Sciences. Piret's research, also in her previous position at the International Centre for Defence and Security, has focused on cyber security and cyber defence, digital policy and transformation, societal security, and comprehensive security and defence. She has extensively published on national, NATO, and the EU cyber security policies and strategies.

Lucy Purdon is Policy Officer with Privacy International responsible for policy development and leading global policy work on cybersecurity and identity. She was also a documentary producer/director and ran filmmaking courses for young offenders in the UK. Lucy has an MA in Human Rights from ICWS, University of London, and a BA (Hons) Film and Video from the London College of Communications.

Allison Pytlak is a Program Manager in the disarmament program of the Women's International League for Peace and Freedom. She has nearly a decade of experience working in arms control and disarmament most recently holding the post of Policy and Advocacy Specialist with Control Arms. She has published on conflict and security issues, as well as the role of civil society in multilateral affairs. She is an adjunct fellow of the Niskanen Centre researching cyber repression of human rights.

Mirva Salminen conducts her doctoral study on digitalisation and cybersecurity in the European High North at the Arctic Centre, University of Lapland, Finland. Previously, she has carried out research for several organizations in both public and private sectors, including universities, research institutes and corporations, publishing primarily on cybersecurity and security commercialisation. Salminen holds M. Soc. Sc. degree in International Politics and B. Soc. Sc. in Political Science, both from the University of Tampere, Finland. Parts of her degrees she has completed in the US and in the UK.

Niels Nagelhus Schia is a senior research fellow and manager for NUPI's Centre for Cybersecurity Studies. Schia focuses on diplomacy and the role of international organizations in global cyber-governance. His publications include 'The Cyber Frontier and Digital Pitfalls in the Global South', 'Horseshoe and Catwalk: Power, Complexity, and Consensus-Making in the UNSC', and *Franchised States and the Bureaucracy of Peace*.

Kunvath Sok works as a project coordinator Cambodia Development Center. He received his Bachelor of Arts in International Relations and Bachelor of Science in Computer Science and Engineering from the Royal University of Phnom Penh in Cambodia.

Anatoli A. Streletsov is Member of the Presidium of the National Association of International Information Security, Doctor of Law and Doctor of Engineering.

Tang Lan is the Deputy Director of Institute of Information and Social Development, China Institutes of Contemporary of International Relations (CICIR). She focuses on the

strategic and policy research about cyber-security and issues related with e-development, and has also published numerous papers on cyber-security, norms of behavior in cyberspace and cyber-terrorism.

Eneken Tikk is Executive Producer of the Cyber Policy Institute and lead of the International Law project of CPI and the Erik Castrén Institute (University of Helsinki). She is the lead author of the Cyber Conflict Factbook and an experienced lecturer and teacher of international law, cybersecurity legislation, cyber diplomacy and cyber conflict prevention.

Tatiana Tropina is an Assistant Professor in Cybersecurity Governance at the Institute of Security and Global Affairs at Leiden University in The Netherlands. Previously, she worked as a senior researcher at the Max Planck Institute for Foreign and International Criminal law in Freiburg, Germany.

Francisco Vera is an Advocacy Officer at Privacy International, working with its international network to build a global privacy movement. He previously worked as Policy Director at ONG Derechos Digitales, and cyber security advisor at the Chilean Ministry of Defence, among other roles related with digital policy and human rights. Francisco holds a LL.B. from Universidad de Chile, and a LL.M. in International Law from George Washington University.

Johanna Weaver is Special Adviser to Australia's Ambassador for Cyber Affairs and Australia's representative to the United Nations Group of Governmental Experts on Responsible State Behaviour in Cyberspace.

Zhang Li is Director of the Institute of Information and Social Development Studies at the China Institutes of Contemporary International Relations (CICIR) in Beijing (a group of experts on crisis management and strategic and policy research on cyber security), and one of the co-sponsors of the Sino-US Cybersecurity Dialogue hosted by CICIR and the Center for Strategic and International Studies (CSIS) in the United States.

Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

INTRODUCTION

Mika Kerttunen and Eneken Tikk

The scene

The title of Raymond Carver's 1981 collection of short stories, *What We Talk About When We Talk About Love*, is inspiring, and, when put as a question, demanding. The very issue of understanding a theme is fundamentally an ontological and epistemological, but also, ultimately, a political one. It is political in the spirit of Schmitt (1932) and Lasswell (1936), drawing lines of demarcation, distilling the acceptable and accepted, segregating *others* from *us*. When talking about international cybersecurity we cannot escape the ontological, epistemological and political issues that underlie and surround it.

Cybersecurity, let alone international cybersecurity, is not rocket science. Rather than being exact, evidenced and prescriptive, the field exists and operates as a political and social construction. At its simplest, international cybersecurity talk speaks of threat vectors and threat actors. To these two forces and factors we seek to apply preventive, defensive, offensive and mitigating measures making cybersecurity problem solving rather than critical (Cox, 1996). Over-cultivation of the security-from attitude easily obscures the security-to dimension (Berlin, 1958). In particular, what and whose security are we talking about? Focusing on being left alone, avoiding interference and keeping out of harm's way, or keeping harm and infraction minimal, and the loud narratives of operations and oppression, eat away at the trust, confidence and self-determination necessary to human and societal development and international peace, security and stability.

Whenever cybersecurity and international politics meet, five themes appear to emerge and re-emerge: information security, cyberspace governance, sovereignty, human rights and the use of force. Here, the simplicity of culprits is replaced by the complexity of relations, the relations between the states, the state and the international community, and the state and the individual.

Information security is a highly contested and confused notion. The whole problem area of cybersecurity turns focuses information and its security, often operationalized as the confidentiality, integrity and availability of information. Accordingly, for some nations the term is all but synonymous with cybersecurity – of something more than information security, perhaps looking beyond mere information towards how information is used, utilized or even exploited. In diplomacy, however, the very notion remains contested, whether information

security focuses (only) on the technical-functional aspects of information security and network protection or (also) on the content of information.

Cybersecurity governance is an emerging theme in international cybersecurity discourse. On the one hand, it represents the increasing pressure on governments – by both their own constituencies and the international community – to take responsibility for national cybersecurity, and, accordingly, contribute to global cyber resiliency. On the other hand, this theme is seen as the sign of a merger between Internet governance and international cybersecurity dialogues. Indeed, a 2015 UNCTAD report listing forty-one ‘international public policy issues’ pertaining to the Internet identifies national, regional and international ‘governance mechanisms regarding cybersecurity’ (UNCTAD, 2015, p. 22).

Sovereignty and human rights have separately and equally become debated and contested issue also in the ICT issues. While some countries have come to emphasise freedom of expression and the free flow of information these technologies offer, other countries stress the challenges to sovereignty the usage of these technologies may pose. Digitalization can be perceived as dangerous. Obviously, how to protect universal and individual human rights is a core question within this often-binary debate.

Increased dependency on information and communication technologies and the proliferation of network exploitation and cyber military capabilities have fed concerns over the use of force in cyberspace. This has given rise to the whole discourse of cyber arms control and the discussion of a special regime applicable to state behaviour in cyberspace. The perceived tendency to securitize cyber policies (Dunn Cavelty, 2008; Stevens, 2017), returns us to Dillon’s (2004) early, Foucauldian questions, ‘How is it that the peace of liberal governance is so suffused with the logics of war?’ ‘How is it that self-regulating freedoms of governance are so intimately correlated with systems of surveillance?’ ‘How is it that such freedoms require extensive apparatuses of security?’ In the field of cybersecurity, for example, international law rather than calling for peace, peaceful settlement and cooperation is often seen to support operations, conflict and war.

The framework

Typologies of action and actors and levels of analysis approaches have been developed and utilized from Byzantium to Prussia, Brussels and Copenhagen. In war and strategic studies, the levels of war from tactical and strategic (Heuser, 2010; Clausewitz, 1832), grand strategic (Liddell Hart, 1954), and operational and technical have been used for academic analyses and contemporary western operational planning (NATO, 2010). Luttwak (1987) presented one of the most encompassing frameworks of analysis comprising of technical, tactical, operational and theatre levels of, in practice, war but also including grand strategy as an encompassing thought and action.

Accordingly, in International Relations and more specifically, in security studies, different levels of analysis are commonly employed. Levels are explicitly used as the framework of analysis or they implicitly constitute a characterization the referent objects of the studies cannot escape. Buzan (1983), in particular, recognized, and later Buzan and Hansen (2009) reiterated, the inter-linkages and tensions across levels of analysis as well as ‘the often-existing movement between different levels of analysis’ (Buzan, 1983, p. 25).

Cyberspace has been operationalized into levels, too. Computer science-based approaches distinguish layers of functionality. Bachman’s Open Systems Interconnection model describes the application, the presentation, the session, the transportation, the network, the logical, the data link and the physical layers (Day, 2008). Libicki (2009) distinguishes the

physical, the syntactic and the semantic layers. American military doctrines have followed the logic but view cyberspace from an operational perspective. For example, the US Army (2010) guidelines distinguish the physical, logical, and social layers, but also the components of geographic, physical network, logical network, cyber persona and persona. A joint level doctrine on cyberspace operations speaks of the physical network, logical network, and cyber-persona (Joint Chiefs of Staff, 2018).

It should be noted that levels of analysis more often than not construct an implicit ontology of the subject matter. Here, ontology refers to the stuff of which something is made of rather than to a deep ontological question of being. Yet, when speaking of levels, we are often referring also to actors. Moreover, as Singer (1961) noticed, a system-oriented analysis may lead to exaggeration of the impact of the (international) system upon national actors and assumes higher level of uniformity from those actors (pp. 78–82).

Accordingly, the notion of *international* can simultaneously be understood as being between (*inter-*), above (*supra-*), beyond (*global*), across (*trans-*) or outside (*foreign*) of nation-states or involving more than one state (*multi-*, *pluri-*), even, although diminishingly in the narrowed communitarian world of Trumps, Xis, Putins, Modis, Erdogans, Salvinis or Orbans, and alike, as *cosmopolitan*. The very notion international, albeit frequently used, is ill fitted as a homogenous level of analysis or a self-evident layer of focus.

The United Nations General Assembly (UNGA, 2015) approaches international security as a world order in which the necessary conditions for the sustainable development of the world are created in its three components – economic, social and environmental. The Russian Ministry of Foreign Affairs (RU MFA, 2016, #13) defines international security being

characterized by the growing use by certain States and organizations of information technologies for military and political purposes, including for actions inconsistent with international law and seek to undermine the sovereignty, political and social stability and territorial integrity of the Russian Federation and its allies, and pose a threat to international peace, global and regional security.

To form a typology of *international cybersecurity* and the framework of analysis for this book the notion of *international* is turned into a noun, an empirical substance matter. Consequently, due to its ubiquitous but at the same time unspecified meaning, *international* as a level is dismissed. Accordingly, this move outlines the levels of cyber activities as technical, individual, organizational, national, regional and global. These levels of activities not having distinct ontological status poses an epistemological challenge: there is no clear location of the international but its movement and impact can be detected. Moreover, when the levels of activities – and analysis – are being operationalized, the cross-level movement disappears. Yet, for the sake of clarity, lines of ontological demarcation are drawn in the following.

The technical level defines the cyber domain as a set of information and communication technologies, networks, infrastructures and resident data. It includes the Internet, computer, radio and telecommunications systems, and embedded processors, controllers and sensors and all the electronic activities and transactions (cf. ITU, 2015; DOD, 2016). The individual and organizational levels refer to corporations and users as subjects and objects in international cyber affairs. Often the issues are guarantees of privacy, economic aspects of information security as well as protection against social, criminal or political exploitation. The national level, obviously, pays attention to national security but also to

the broader issues of societal development affected by intentional policy and legislative moves and industrial innovations. The regional level introduces the traditional issues of cooperation and conflict. In cyber affairs the issues range from standardization and regulation to inter-state peace and stability. Here, for example, confidence-building measures include cooperative mechanisms to prevent the escalation of conflicts and, ultimately, war. Finally, the global level adopts a universal perspective where the paramount questions become equality, peace, stability and world order. To address global *problematique*, international law and other normative mechanisms come to play an important role. However, similarly to all other levels, the global level is not insulated from the dynamics of, and in between, other levels or areas.

During the last decade, cybersecurity has moved from being an expert issue to being an everyday issue, widened from a technical issue to a political and military one and expanded to cover high as well as local politics. The discourse can be read about as a) the sum of all global cybersecurity fears, b) as a combination of national cybersecurity concerns, or c) strictly a matter of peace or war.

This book combines a nuanced reading of the *international* with the established focus on peace and security. International cybersecurity in this handbook refers to *transnational or cross-border interaction and effect in and across the levels of cyber activities that are considered to impact international peace and security*. It analyses the causality between factors (*interaction* and *activities*) and functions (*effect* and *impact*) and recognizes both threatening and enforcing effects and impacts. Most importantly, the handbook seeks to establish the existence or non-existence of actual impact that the examined activities and their interaction have on international peace and security.

This research interest stems from the United Nations Charter. The United Nations (UN) is the guardian of international peace and security. The peoples of the United Nations, by signing the UN Charter, have determined ‘to ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used, save in the common interest’ (UN, 1945, preamble). Moreover, international disputes are to be settled ‘by peaceful means in such a manner that international peace and security, and justice,’ will not be endangered (UN, 1945, 2(3)). Do cyber issues, problems and breaches constitute a threat to the peace, breach of peace or an act of aggression potentially leading to the UN Security Council to determine such a situation to exist and take corrective collective measures?

In international cybersecurity discourse such a strict emphasis on peace and security has not been followed. A motley crew of cybersecurity themes, currently discussed in various international cybersecurity venues, neither necessarily nor primarily constitutes *international security* concerns. Yet, if any cybersecurity problem can and will be turned into an international cybersecurity question, we won’t be able to differentiate serious from banal, will get false and dangerous expectations of roles and responsibilities and will kill the promise of information and communication technologies with the weight of domestic and national security.

Furthermore, the use, if not the meaning, of the notions such as ‘war’, ‘confidence-building measures’, ‘international law’, ‘deterrence’ or ‘intervention’ have been expanded, even stretched. Amidst this freedom of expression, we should critically ask and examine whether it would be useful to limit references to war, peace and international security in the ICT environment to the questions of war, peace and survival, death and destruction. This U-turn could free us to focus and solve every-day problems of cybersecurity without the assumptions, claims and limitations of high politics.

To capture the political, legal and academic discourse of international cybersecurity, this book examines issues beyond a narrow reading of international peace and security in the ICT environment. We follow the spirit of the UN Security Council – at its best, we dare to claim – and regard issues of development, human rights and justice of essential importance also for international cybersecurity. Accordingly, wider national, organizational or individual readings have been applied.

Within this framework, the *Handbook of International Cybersecurity* allow us to visit a wide variety of themes and topics that have been introduced to this scene, without necessarily justifying their relevance to, or relationship with, international peace and security. We shall introduce paths that threaten peace and security. Most importantly, we shall examine measures that could increase national and international cybersecurity and strengthen international peace and security.

The Routledge Handbook of International Cybersecurity

In this book, we ask ‘What is international cybersecurity?’ We examine themes claimed to be essential to international cybersecurity. We offer views on what cybersecurity issues can affect international peace and security, and how; we offer views on measures and mechanisms that may promote international peace and security, including stability in cyberspace.

We do not take a stand on whether cybersecurity should be approached as being or becoming an objective truth or constructive, intersubjective process (Stevens, 2017), but leave that to be tackled, or not, by individual authors. Thus, some authors may question the realist emphasis on cybersecurity, its goals, objectives and methods, and pay attention to the wider contexts, purposes and approaches as well as the subjective or intersubjective nature and processes of the field – others may not. This diversity of epistemic approaches, in our minds, reflects the very nature of cybersecurity, even how underdeveloped the discipline, and the politics of it, is.

The *Routledge Handbook of International Cybersecurity* is organized into four parts. We begin with conceptual analysis. Among other things, the notions, concepts and principles of conflict, securitization, governance and human rights are discussed in the framework of cybersecurity and international cybersecurity. The second part focuses on a number of challenges to secure and peaceful cyberspace. Here, we have deliberately tried to avoid the rather usual accounting of threat actors and threat vectors (e.g. the typology of hacking, cybercrime, cyberterrorism and nation-state cyber operations) but asked the contributors to offer broader, global and societal perspectives and consider the impact on international peace and security. The third part introduces regional, sub-regional and national views. Here, the chapters analyze issues such as cyber capacity-building and national cybersecurity strategies but also offer normative standpoints on international cyber affairs. The fourth part analyses a variety of political, legal and technical solutions countries, the international community and communities of interests have come up with to solve or mitigate security issues and concerns. The *Handbook* ends with an analysis of our discussion of international cybersecurity.

The reader will notice that many chapters are thematically interlinked. Here we mention but few: securitization (Dunn Cavelty) and the development of cyber military capabilities (Salminen & Kerttunen; Pernik); vulnerabilities (Martin; Butrimas), cyber conflict (Mitchell; Demchak), and operations (Libicki; Flyktman, Huhtinen & Koreman); international law (Brown), principles of international law (Park & Chung), the United

Nations Security Council (Tikk & Schia), the Trump administration cyber policy (Lewis), and human rights (Pytlak); regional views (Lim & Sok; Vera & Purdon; Oyelola), and capacity-building (Amazouz; Contreras & Barret); the roles of technical communities (Hinojosa, Aiken & Huriel), industry (Buzatu), and diplomacy (Feakin & Weaver); global governance (Lan; Tropina), national views and ambitions (Zhang; Ang; Lewis; Krutskikh & Streltsov), confidence-building measures (Meyer), and export controls (Claussen). Similarly, deterrence, development and the 'UN GGE' run across the chapters, where traces of espionage can also be detected. Private space and public sphere, open and closed, security and resilience appear variously in the chapters. Indeed, we hope that the plurality of views, and the cross-cutting elaborations, offers several ways to read, and become inspired by, the *Handbook*.

To conclude, it should be noted that the main contested and conflictual issues, as well as many of the proposed and implemented measures, stem from the 'pre-cyber' era. This bears witness to both the durability and applicability of, for example, international law, diplomacy and confidence-building measures in cyber matters, but also of their impotence in solving fundamental disputes among states, nations and people. We may critically comment that the international community has not been able to provide alternative approaches to such a multifaceted and boundary-crossing issue as international cybersecurity. As contemporary cyber-politics resembles a distorted auction where the lowest bidder wins, maybe it is time to regain some high ground and restart reading and teaching international law at its best – the UN Charter.

Second, we observe in the use of ICTs an oscillation between an emphasis on domestic order and cyber operations. Similarly to DeVisscher's (1968, p. 86–87) analysis of the Cold War, we notice that national policies and actions are being characterized by a general 'sense of insecurity' now stemming from and intensified by enhanced connectivity and the lack of proper security and resilience. Moreover, amidst inflicted superpower relations of the 2010's, worldwide cybersecurity has turned into identity politics. The values and norms being promoted present particular group identities, which, in turn, downgrades universal approaches and upgrades unilateral action and insulated cleavages of governance.

We nevertheless read a common appetite for a rule-based public order in and for cyberspace. Governments, corporations, non-governmental organizations and individuals are looking for ways to keep the promise of positive *opportunities* alive – some perhaps more egoist and hypocritical than altruistic and conscious.

Overall, we tend to recognize different calls for national resilience, and even caution when dealing with new and vulnerable technologies. This emphasis on national measures may appear surprising in a book on international affairs. Given our experience, exchanges and research, we find this to be honest. Cybersecurity begins at home, and international cybersecurity can best be promoted by domestic action: governments of the world, take responsibility. Given the current deadlock between the superpowers, the national interests of less eager-*operational* or muscular-*oppressive* states can perhaps best be (inter-nationally) satisfied by regional, sub-regional or bilateral arrangements – nations holding their heads high and refusing to play the game dictated by Moscow, Beijing, or Washington, DC. Paraphrasing Gopalkrishna Gandhi (2019), disobeying the instructions these three capitals with respect to cyber affairs enables us to remain civil, civilised and civilising.

Third, we detect structural tensions among global, regional and local cyber agendas. While governments are keen to employ advanced ICTs and 'emerging technologies', they are still medicating than curing the inherent vulnerabilities and resulting problems. Tensions

arise not only between developing countries and the developed ones but also between national centres and peripheries – the digital haves and have-nots. Similarly, as with acquiring a taste for fine wine, venison and Scotch, the elites of the developing countries are unquestionably accepting Western patterns of online behaviour.

Finally, we also want to pay attention to epistemological questions (which many Realists abhor): ‘How do you know what you are claiming?’ For example, how do we know of, say, cyber deterrence (which many of the chapters refer to); why are we talking about norms, rules and principles (similarly noted by many of our contributors); or, why are we less knowledgeable about, say, the cybersecurity dilemma than about the responses and countermeasures (which some countries are promoting)? How do we know which numbers and evidence we can trust? This is not a post-truth but a pre-methodological question concerning credibility.

We hope that the questions we have posed and the answers the individual authors have promoted stimulate methodologically credible research, truthful policy-making and, most of all, independent and critical thinking at home and in international cyber and information security venues.

References

- Berlin, I. (1969, orig. 1958) *Two Concepts of Liberty*. In *Four Essays on Liberty*. Oxford, Oxford University Press.
- Buzan, B. (1983) *People, States, and Fear*. Brighton, Harvester Wheatsheaf.
- Buzan, B. and Hansen, L. (2009) *The Evolution of International Security Studies*. Cambridge, Cambridge University Press.
- Carver, R. (1981) *What We Talk About When We Talk About Love*. New York, Alfred A. Knopf.
- von Clausewitz, C. (1991, orig. 1832) *Vom Kriege*. Köln, Ferd. Dümmler Verlag.
- Cox, R. (1996). *Approaches to World Order*. Cambridge, Cambridge University Press.
- Day, J. (2008) *Patterns in Network Architecture: A Return to Fundamentals*. Boston, Pearson Education.
- DeVisscher, C. (1968) *Theory and Reality in Public International Law*. Princeton, Princeton University Press.
- Dillon, M. (2004) The security of governance. Available from: www.academia.edu/3893984/The_Security_of_Governance [accessed 30 January 2018].
- Dunn Cavelt, M. (2008) *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Abingdon, Routledge.
- Gandhi, G. (2019) It's all about love. *India Today*. (19 August), 24–26.
- Heuser, B. (2010) *The Evolution of Strategy*. Cambridge, Cambridge University Press.
- International Telecommunications Union (ITU) (2015) *Measuring Information Society Report 2015*. Geneva, ITU.
- Joint Chiefs of Staff (2018) *Cyberspace Operations*. (8 June).
- Lasswell, H. (1936) *Politics: Who Gets What, When, How*. Chicago, Chicago University Press.
- Libicki, M. (2009) *Cyberdeterrence and Cyberwar*. Santa Monica, RAND Corporation.
- Liddell Hart, B.H. (1954) *Strategy*. London, Faber & Faber.
- Luttwak, E. (1987) *The Logic of War and Peace*. Cambridge, MA, The Belknap Press of the Harvard University Press.
- The Ministry of Foreign Affairs of the Russian Federation (RU MFA) (2016) *Doctrine of Information Security of the Russian Federation*.
- MITRE Corporation (2010) Cybersecurity governance. Available from: www.mitre.org/publications/technical-papers/cyber-security-governance [accessed 30 January 2018].
- North Atlantic Treaty Organization (NATO) (2010) *Comprehensive Operations Planning Directive*. Mons, Allied Command Operations.
- Schmitt, C. (1932) *The Concept of the Political*. Chicago, Chicago University Press.
- Singer, J.D. (1961) The level-of-analysis problem in international relations. *World Politics*, 14(1): 77–92.
- Stevens, T. (2017) *Cyber Security and the Politics of Time*. Cambridge, Cambridge University Press.
- United Nations (1945). *The Charter of the United Nations*.

- United Nations Commission on Science and Technology for Development (2015). Mapping of international Internet public policy issues. Report E/CN.16/2015/CRP.2. Available at: https://unctad.org/meetings/en/SessionalDocuments/ecn162015crp2_en.pdf [accessed 2 August 2019].
- United Nations General Assembly (2015) Transformation of our world: An agenda for sustainable development for the period up to 2039. A / RES / 70/1.
- United States Army (2010) Cyberspace Operations Concept Capability Plan 2016–2028. *TRADOC Pamphlet* no. 525–7–8, 8–9.
- United States Department of Defense (DOD) (2016) *Strategy for Operations in the Information Environment*, 3.
- United States Department of Defense (DOD) (2018) *Cyberspace Operations*. Joint Publication 3–12, I–2–I–4.

PART I

Concepts and frameworks

Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

1

CYBERSECURITY BETWEEN HYPERSECURITIZATION AND TECHNOLOGICAL ROUTINE

Myriam Dunn Cavelty

In 2006, detecting ‘great difficulties for theoretical adaptation and application in analyses of the complexities of the emerging new digital world’, Eriksson and Giacomello (2006, p. 236) observed that the political sciences were struggling to apply their varied theoretical toolbox to the topic of cybersecurity. More recently, however, changes in the empirical phenomenon and an increasing diversity in the theoretical landscape have made it more viable and more opportune to use theory to help explain different facets of the phenomenon. As a result, research that uses international relations (IR) theory for the study of cybersecurity is no longer quite like a unicorn; mystical, rare and extremely hard to find.

The focus of this chapter is a type of cybersecurity research in the IR sub-discipline security studies that applies variations of the Copenhagen School’s securitization theory to cybersecurity (prime examples: Eriksson, 2001; Dunn Cavelty, 2008; Hansen & Nissenbaum, 2009; Lawson, 2013). Securitization signifies the representation of a fact, a person, or a development as a danger for the military, political, economic, ecological, and/or social security of a political collective and the acceptance of this representation by the respective political addressee (Buzan et al., 1998). The successful securitization of a topic justifies the use of all available means to counter it – including those outside the normal political rules of the game. Therefore, a strongly mobilizing discursive justification for this extraordinary situation is made in the political process. This happens above all in the narrative representation of great danger threatening objects of value.

Given these theoretical underpinnings, the Copenhagen School focuses mainly on official statements by heads of state, high-ranking officials or heads of international institutions (Hansen, 2006, p. 64). What a focus on elite speech acts ignores, however, is how these discursive practices are facilitated or prepared by practices of actors that are not so easily visible. The social competition for the definition of reality is not only – and above all only in the final stages – held in the open political arena. Empirical analysis reveals that there are always state and non-state actors ‘under the radar’ – i.e. specialized bureaucratic units, consultants or other experts – who have the capacity to establish ‘the truth’ about certain threats, thus pre-structuring the discursive field in relevant ways (Huysmans, 2006, p. 72; Léonard & Kaunert, 2011).

Taking this as a starting point, a second type of literature moved away from speech acts to see cybersecurity as a product of the interaction of technologies, processes, and everyday

practices. It pays particular attention to how a variety of actors uses different representations of danger to create or change different political, private, social, and commercial understandings of security in selected public spheres. In addition, this type of literature gives more weight to material aspects of the issue (examples: Stevens, 2016; Balzacq & Dunn Cavelty, 2016; Collier, 2018; Shires, 2018). It takes the possibilities and constraints of the technical environment seriously by recognizing that the political reading of cybersecurity cannot be divorced from the material realities of computer disruptions and knowledge practices in technical and intelligence communities, which shape the field constantly through their everyday offensive and defensive actions.

This chapter makes an argument that cybersecurity politics is best understood as running on a continuum between securitization tendencies and technological routine depending on the context and sub-issue under scrutiny. There are three sections. In the first, securitization theory as an important part of European ‘critical security studies’ is introduced, to give the reader an overview over the key concepts and theoretical assumptions of this approach. In the second, the challenges of applying securitization theory to cybersecurity are discussed by pointing out a few specificities of the issue. In the third, the chapter shows how securitization theory has evolved to become more applicable to cybersecurity. An argument for the combination of approaches is made by highlighting the seminal work of Hansen and Nissenbaum (2009) who describe a multifaceted ‘grammar of security’ for the cybersecurity sector.

Securitization Theory and beyond

Securitization Theory, also called Copenhagen School, was developed in the 1990s as part of a critical turn in security studies in Europe. While some scholars sought to keep security studies narrow as ‘the study of the threat, use and control of military force’ (Walt, 1991, p. 22), other scholars soon began to expand the scope of security to non-military issues and subsequently moved away from a sole focus on state actors (Baldwin, 1995). Whereas security studies in the United States continued to follow a path of mainly positivist, neo-realist inspired research answering ‘why’ questions, Europe chose to focus more on issues of a reflexive nature, engaging with so-called ‘how possible’ questions (Wæver & Buzan, 2015). Rather than believing that there is a social reality that can be measured with methods mirroring those used in the natural sciences as positivists do, these approaches seek to understand the construction of political issues and their social consequences, often using constructivist or post-structuralist thought as a starting point. While the label ‘critical’ means different things to different scholars (Mutimer et al., 2013), they share an interest in taking up various unquestioned and taken-for-granted aspects of security. By opening them up for analytical and normative inquiry, they initiated important conceptual debates on the deeper politics of security.

Securitization looks at the formation of security policy agendas, arguing that problems become a security issue not because an objectively measurable, existential threat exists, but because key actors successfully *present* and *establish* issues as such a threat (Buzan et al., 1998). Wæver and Buzan offer the following definition of securitization as ‘the discursive process through which an intersubjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with the treat’ (Buzan & Wæver, 2003, p. 91). Overall, the study of securitization therefore aims to gain an understanding of who securitizes (the actor) which issues (the threat subject), for whom or what (the referent object), why (the intentions and purposes), with what results (the outcome), and under what conditions

(the structure) (Buzan et al., 1998, p. 32). The overall take on security is based on speech act theory as developed by Austin (1962) and Searle (1969), which claims that the use of language is a performative act. Security speech acts are significant utterances in a security framework by actors that are in a position to 'define' security and shape responses to envisaged threats (Strizel, 2007, pp. 360f).

By choice, securitization theory deals with a type of security that is discursively tied to the highest possible political stakes, since it is about existential threats to the survival of the state and its society. Therefore, invoking security is a powerful mobilizer that can help legitimize extraordinary responses and undemocratic procedures (Wæver, 1995; Huysmans, 2008). However, many of the current security issues in the West are hardly about the outright survival of the state or society but characterized by the risk of (wilful) disruption of modern life in open, liberal societies. Such conceptualizations are empowering a range of specific government rationalities like the permanent surveillance of populations, precautionary arrests of suspects, or pre-emptive invasions of foreign countries (Aradau & van Munster, 2007). When focusing on security that is no longer primarily about threats and battles against an enemy, but is characterized by an inward-looking narrative about vulnerabilities, it becomes necessary to question the perception of security as 'exceptional' and linked to 'extraordinary' means.

In line with these observations, scholars from the *Institut d'Etudes Politiques de Paris* challenged the Copenhagen School's conceptualization of security from the moment of its inception. This 'Paris School' criticized that by focusing exclusively on discursive practices, the Copenhagen School overlooked the important *non-discursive practices* of security formation by agencies in the security domain (Bigo, 1998). Following Bourdieu and his work on social fields (Bourdieu, 1993), the Paris school's approach focuses mainly on the action of those actors who are endowed with both the symbolic capital and the capacity to inter-link heterogeneous discourses by establishing 'the truth' about certain security threats. The securitization process cannot be reduced to simple rhetoric, but implies extensive mobilization of resources to support the discourse. New practices and institutions need to be created to deal with the quasi-ubiquitous danger that the 'new' threats constitute (Huysmans, 1998; Bigo, 1994).

When engaging with the political handling of such issues, the research focus inevitably shifts to everyday security practices of less traditional security actors such as civil protection or police agencies (Huysmans, 2006; Hagmann & Dunn Cavelty, 2012). In this view, security is not only about the exceptional but also about routine processes in bureaucracies (c.a.s.e. collective, 2006, p. 469; Lobo-Guerrero, 2008). This type of scholarship accepts more amorphous and ambiguous characteristics of national security. Its referent objects populate a national security spectrum that connects global threats right down to personal safety. Its referent object is often not the population or life more broadly but technical and social systems that are designated vital to collective life. The sources of insecurity – classically, the 'enemy' – are moved to the background, as the stability of technical and societal systems becomes a main aim of security interventions.

Securitization Theory and cybersecurity

For many years, political aspects of cybersecurity were discussed almost exclusively in policy-oriented publications originating in the US (for example, Alberts & Papp, 1997; Arquilla & Ronfelt, 1997). The two main questions this literature tackles are 'who (or what) is the biggest danger for an increasingly networked nation/society/military/business

environment' and 'how to best counter the new and evolving threat'. Predominantly, this literature follows a technologically deterministic reasoning, which assumes technology is shaping society with society or politics having little power to shape technologies in turn. In line with this, the information age is touted either as a great, world-changing opportunity (Toffler, 1981; Drucker, 1989) or as a certain factor for doom and destruction (Clarke & Knake, 2012). In line with this, the US policy discourse and the publications looking at cybersecurity at the intersection to national security more often than not presented large-scale, devastating cyberattacks under a 'not a matter of if, but when' logic.

As a reaction to what seemed like inflationary and sensationalist danger hyping, scholars began applying the Copenhagen school's body of thought to cybersecurity to gain a better understanding of why the threat was constructed this way and what the consequences of such a construction were. The prime question this literature asks is whether cybersecurity is securitized or not. For Copenhagen scholars, security, with the sense of urgency that it implies, is deeply transformative of liberal democratic ideals of deliberation by foreclosing contestation and open-ended debates in politics. Subsequently, scholars have pondered how such a removal of proper politics from government could be prevented or reversed, in other words, how issues could be *desecuritized* (Hansen, 2012; Aradau, 2004). They believe in a (normative) commitment to 'normal politics' and the democratic responsibility and accountability that come with it.

What becomes apparent, however, is how difficult it is to answer this very question if we apply the Copenhagen School's toolset to cybersecurity. Without a doubt, cybersecurity is considered and actively pursued as an (inter-)national security issue worldwide. Therefore, it must have been securitized; at least if we apply the common sense yardstick that issues are securitized when they are included in national security strategies and related documents and/or fall under the purview of a state's security apparatus. However, what seems a straightforward observation is far less clear-cut under scrutiny, not least because of ambiguities in the theory.

In their 1998 book, Buzan et al. briefly touch upon the cyber issue and make an interesting observation:

Securitization is not fulfilled only by breaking rules (which can take many forms) nor solely by existential threats (which can lead to nothing) but by cases of existential threats that legitimize the breaking of rules. Still, we have a problem of size or significance. Many actions can take this form on a small scale – for example [...] the Pentagon designating hackers as 'a catastrophic threat' and 'a serious threat to national security' [...] which could possibly lead to actions within the computer field but with no cascading effects on other security issues.

(Buzan et al., 1998, p. 25)

Though they do not elaborate why they consider these 'actions within the computer field' to be about breaking rules and they are clearly wrong about the non-existing 'cascading effects on other security issues', they still raise the important question of a security 'threshold'. According to them, it should not be set too low, unless we want a too many issues to be considered securitized.

Hansen and Nissenbaum (2009) have a surprisingly different take on this. They claim that

cyber security *is* successfully securitized as evidenced by such institutional developments as the establishment of the Commission on Critical Infrastructure Protection by President Clinton in 1996, the prominent location of cyber security within the Department

of Homeland Security, President Bush's formulation of The National Strategy to Secure Cyberspace in 2003, and the creation of a NATO backed cyber defense center in Estonia in 2008.

(Hansen & Nissenbaum, 2009, p. 1157, italics in the original)

Further on in the text, they write that 'the ability of Estonian securitizing actors to have the attacks [they are referring to the 2007 DDoS-attacks on Estonian websites] accepted as 'the first war in cyberspace' and to have them prominently covered by the world press makes for at least a partially successful case of cybersecuritization' (ibid., p. 1169). By implication, the 'proof' for successful securitization is institutional reactions (of all sorts) and the persuasion of an unnamed audience plus the media – which therefore seems to be treated as an audience somewhat untraditionally. Clearly, this is an extremely low benchmark for something to be securitized. In fact, if any kind of policy reports or institutional responses are proof for the successful securitization of an issue, securitization is starting to encompass everything that happens in the policy processes. While this might be a deliberate choice to make depending on what we want securitization theory to be, it comes with certain 'cost', like losing the initial focus of the theory.

Others come yet to different conclusions and call the debate on cyber risks an example of a failed securitization (Bendrath, 2001, p. 79; see also Dunn Cavelty, 2008; 2012). When not only focusing on threat representations – which are indeed full of military analogies and 'multi-dimensional cyber disaster scenarios' (Hansen & Nissenbaum, 2009, p. 1164) – but at the characteristics of the actual countermeasures and practices adopted to counter cyber-threats, the significant difference between the content of the threat representations and the selected policies is striking. For example, the outcome of ten years of discussion and almost five years of reforms, presented by Clinton in the National Plan for Information Systems Protection in January 2000 (Clinton, 2000), consisted of three approaches: law enforcement lead, private-public partnerships, and private and public self-help. At its core, we find the strategy of preparation, meaning the preventive protection of critical infrastructures by technical means (Dunn Cavelty & Suter, 2012). None of them are exceptional or about breaking rules, quite the opposite.

In addition, rather than seeing the removal of the issue from political processes, we can observe democratic deliberations over many years. On the one hand, law enforcement agencies emphasized their view of the risk as 'computer crime,' while on the other hand, and more importantly, the private sector that runs critical (information) infrastructures perceived the risk as consisting primarily of a local, technical problem or as economic costs (Dunn Cavelty, 2008; also Bendrath, 2001; 2003). When there are concurrent discourses and viewpoints, the actual selection of policy instruments depends upon more than securitization logic, like the ability to dominate the discourse with the help of available resources or other factors such as cultural, legal, or technical norms, because they restrict the number of feasible strategies available for selection.

As for the role of the military and the intelligence community, an expansion of the offensive toolset both in theory and practice could be read as an increasing securitization (or rather militarization) of cyberspace. Then again, the addition of cybertools to the military (and intelligence) arsenal could also be framed as a normalization of information technology in the national security context. In fact, no securitization moves were ever necessary to turn 'cyberspace' into an additional domain of warfare. The link between information technology and national security was firmly established in military writings in the time after the Second World War (see for example Rona, 1976; Edwards, 1996) and remained uncontested.

The US military and its strategists treated information technology like other technologies before it mainly as a force enabler, while at the same time keeping an eye on how the evolving information domain was challenging the war fighting capabilities of the US military.

Last, military analogies like cyberweapons, cyberoffence, cyberdefence are just different words for well-known computer tools and information assurance concepts. For example, a cyberweapon is simply software, and software has particular characteristics, many of which are diametrically opposed to the image of a weapon that can be directed at a target of choice with foreseeable effects (Stevens, 2018). Cyberdefence in turn may suggest military personnel doing martial things, but military networks are protected by the same basic concepts as any other type of network; and we are back to the everyday, normal, unexceptional practices of IT security professionals.

‘Little security nothings’ and a focus on security practices

What the previous section showed is how different perspectives or arguments can be used either for or against the successful securitization of cyberspace. The issue seems directly related to the issue matter. What exactly are we looking at? The following observations expose some of the difficulties that come with the label ‘securitized’ as they point to different degrees of securitization, multiple framings and multiple audiences, and a set of different and ‘unexceptional’ set of countermeasures.

First, when IT-issues were put on the political agenda in the 1980s, there was a national security connotation to it from the outset (Dunn Cavelty, 2008) – so that it could be argued that an actual securitization move was not even necessary, because the issue was never anything *else* than securitized. Then again, the security connotation has changed and recently intensified, with a lot of activity in the military and the intelligence community, so that it could also be argued that the issue is either ‘more’ securitized or differently securitized today.

Second, the cybersecurity danger discourse is about a diverse set of threat forms: ranging from computer viruses and other malicious software to cybercrime activity to the categories of cyberterror and cyberwar. Indeed, judgments on the state of cybersecurity-securitization directly depend on how the issue is defined and delineated. Therefore, clearly establishing the empirical object is a first necessary step in any such undertaking. It seems fruitful to advocate a use of cybersecurity that largely overlaps with the common understandings and practices of experts with discursive powers in the field. This ‘praxicological’ approach takes into account practices directly labelled (relevant to) cybersecurity, but also, within reason, more contested indirect practices, that have bearing on cybersecurity or are affected by cybersecurity. Under scrutiny, we see that each sub-issue is represented and treated differently in the political process and at different points in time. In other words, multiple actors use different threat representations employing differing political, private, societal, and corporate notions of security to mobilize (or de-mobilize) different audiences. Which aspect is it that we should focus on if we want to see whether the issue has become securitized? Is it sufficient if one part is securitized or does it need to be all of them? Cybersecurity as a grab-bag concept for a heterogeneous set of threats and practices makes it hard to make general claims about the entire range of sub-issues it contains.

Third, existing cybersecurity-policies contain an amalgam of measures, tailored to meet these different, and at time conflicting security needs. However, even though an existential threat is frequently invoked, cybersecurity practices are also and often even predominantly about technical, normal, and routine practices like mitigating risks to information networks by technical (and occasionally organizational) means – also in the military domain.

While there are some exceptional measures we can identify, depending on how we define cybersecurity, it remains unclear whether exceptionality is a dominant or marginal aspect of policy responses and countermeasures. Even if we define securitizing practices broadly, as not only as emergency measures but also as extraordinary, unprecedented or unusual ones (cf. Léonard, 2010, pp. 237f.), cyber-security practices elude this categorization.

Given its heterogeneous political manifestations, cybersecurity emerges as an empirical challenge to linguistic approaches to securitization. However, the challenge does not end there. Even when employing an arguably better-suited sociological approach that is sensitive to policy tools and their (potential) securitizing effects (cf. Balzacq, 2008), cyber-security emerges as a strange animal. It does not quite fit any of the existing and pre-used 'security'-categories, neither conceptually or theoretically. Because of persuasive threat clustering, it has become more than just a technical issue, but in many ways, it is often handled free of exceptional or extraordinary measures. However, the verdict that cybersecurity is *not* securitized or is an instance of failed securitization is both counter-intuitive and analytically unsatisfactory, since the national security connotation has become so strong in the last few years.

In the last couple of years, various scholars have tried to specify and improve the analytical salience of first-generation securitization theory by developing more elaborated theoretical and analytical models for studying the processes of securitization. Several of these 'additions' are useful to analyse aspects of the cyber-discourse. Some scholars have noted that the process of securitization in a given socio-political community is not restricted to one setting and one type of audience only, but several, overlapping and multiple (Balzacq, 2005; Léonard & Kaunert, 2011), which could take into account the multiple framings to be observed in the cyber-domain. Others have added a temporal aspect to move away from the Copenhagen school's fixation with a particular, transforming (and performing) moment (the Speech Act) (Salter, 2008, pp. 575ff.), which could help to understand the 'history' of cyber-security, with its near thirty years of (failed) securitization moves. Also, others have tried to allow for a better grasp of the continuum along which decision makers categorize challenges, thus adding 'degrees' of securitization – or degrees of successful securitization moves (Haacke & Williams, 2008; McDonald, 2008), which can help us understand different 'strength' of securitization within the same issue-complex. Also importantly, there are different political functions of security utterances in cybersecurity, as Vuori has shown (2008, p. 76), like putting an issue on the political agenda, or, in the case of cyber, securing funds.

Many of the above scholars inadvertently or consciously move away from the linguistic approach towards a sociological approach and a focus on security practices. Balzacq has noted that it is useful to 'focus on the functions and implications of policy instruments used to meet a public problem' (2008, p. 75) 'rather than investigating the construction of threat at the level of discourse' (ibid.). With this shift in focus, the question of whether something has been securitized or not moves to the background, and the effects of security practices comes into focus. Huysmans, following Bigo, argues that modern type of political governance is typical for non-discursive, constantly evolving security practices set up by technocrats and experts ('banal, little security nothings'). These daily practices of security governance, in which bureaucracies and experts define new security issues and link them to potentially dangerous classes of citizens or categories of behaviour, formulate the security management of these issues (Huysmans, 2006, p. 72).

In a seminal text, Hansen and Nissenbaum (2009) operationalize this diversity of cyber-security practices. They identify three traits specific to the logic of security in the 'cyber'-sector. First, hypersecuritization, which refers to the use of 'multi-dimensional cyber disaster

scenarios' to create a sense of urgency (Hansen & Nissenbaum, 2009, p. 1164). Second, everyday security practices, which refer to the mobilization of the individual to perform cyber-hygiene practices as part of the national security enterprise. And third, technification, which is about the special status given to technological expertise in the discourse.

By extending on Buzan's conceptualization of hypersecuritization (2004), they point to the mobilization through narrated, potential, future catastrophes of instantaneous, cascading destruction in cybersecurity, coupled with the absence of historical incidents of the same magnitude (Hansen & Nissenbaum, 2009, pp. 1163–1165). The cascading nature of networked mega-catastrophes, coupled with the 'not a question of if but when' logic is used to generate a strong urgency and impetus for action. This type of reasoning has been the focus of most cybersecurity research using the securitization framework.

Second, everyday security practices are a specific grammar of the cybersecurity sector, in that securitizing actors mobilize individuals' experiences of insecurity for both ensuring their partnership and compliance, but also to connect hypersecuritizing scenarios to their lived experiences (*ibid.*, p. 1165). Individual security practices thereby get cast as both a potential remedy of insecurity (i.e. individuals as 'responsible' partners), as well as a driver of insecurity (i.e. individuals as threats) to the network, and consequently to the larger referent object (state, society).

The third element, technification, acknowledges to the cybersecurity discourse's particular construction of audience-expert subject positions. It thus refers to the use of speech acts that construct the issues as reliant upon technical knowledge and the supposition that this serves a political and normatively neutral agenda (*ibid.*, p. 1167). This technical constitution of the cybersecurity discourse legitimizes technical experts, rather than other political actors, to address cyberinsecurity. As Hansen and Nissenbaum state, technification is a powerful logic of security with strong undemocratic tendencies (*ibid.*, pp. 1167–1168). By making cybersecurity an issue of the 'genius few', technification makes contestation from those with less technical expertise hard or makes it easy for those with the expertise to discredit others that do not have it. In addition, the power of technical expertise comes with a claim of being 'neutral' or 'a-political', and hence, as more valid than anything that seems emotional or based on morals. This is the probably least analysed yet most important aspect of cybersecurity today that should get more attention from research.

Conclusion

Cybersecurity is as an issue of top priority discussed in the national security circles of many countries. Clearly, it has been securitized. But has it really? Yes, it is securitized if we consider things included in national security strategies and similar documents, or things very actively discussed by actors in security politics to be securitized. But when applying the analytical tools of securitization theory, a picture that is far less clear emerges. First, even though an existential threat is frequently invoked, actual cybersecurity practices are often about technical, unexceptional practices like mitigating risks to information networks by technical (and occasionally organizational) means. Second, multiple actors use different threat frames employing differing political, private, societal, and corporate notions of security to mobilize (or de-mobilize) different audiences. Cybersecurity-policies contain a similar amalgam of countermeasures, tailored to meet these different security needs.

Cybersecurity emerges as empirical challenge to securitization theory in multiple ways. By examining previous work on the securitization of cybersecurity and by establishing why the cyber-in-security discourse is so challenging to get a grip on, this chapter has shown

which aspects of securitization theory provide which kinds of insights into the processes behind cyber-(non)-securitization. In particular, by moving away from a focus on ‘security utterances’ towards a more systematic inclusion of ‘security practices’, cybersecurity can be analysed in its variety and additional security dynamics beyond the direct focus of securitization theory can be captured.

References

- Alberts, D.S. & Papp, D.S. (eds) (1997) *The Information Age: An Anthology of Its Impacts and Consequences* (Vol. I). Washington: National Defense University Press.
- Aradau, C. (2004) Security and the democratic scene: Desecuritization and emancipation. *Journal of International Relations and Development*. 7 (4): 388–413.
- Aradau, C. & van Munster, R. (2007) Governing terrorism through risk: Taking precautions, (un) knowing the future. *European Journal of International Relations* 13 (1): 89–115.
- Arquilla, J. & Ronfeldt, D.F. (eds.) (1997) *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, RAND.
- Austin, J.L. (1962) *How to Do Things with Words*. London, Oxford University Press
- Baldwin, D. (1995) Security studies and the end of the cold war. *World Politics*, 48(1): 117–141.
- Balzacq, T. (2005) The three faces of securitization: Political agency, audience and context. *European Journal of International Relations*. 11 (2): 171–201.
- Balzacq, T. (2008) The policy tools of securitization: Information exchange, EU foreign and interior policies. *Journal of Common Market Studies*. 46(1): 75–100.
- Balzacq, T. & Dunn Cavelt, M. (2016) A theory of actor-network for cyber-security. *European Journal of International Security*. 1(2): 176–198.
- Bendrath, R. (2001) The cyberwar debate: Perception and politics in US critical infrastructure protection. *Information & Security: An International Journal*. 7, 80–103.
- Bendrath, R. (2003) The American cyber-angst and the real world – any link? In Latham R. (ed.), *Bombs and Bandwidth: The Emerging Relationship between IT and Security*. New York, The New Press, pp. 49–73.
- Bigo, D. (1994) The European internal security field: Stakes and rivalries in a newly developing area of police intervention. In Anderson, M. & den Boer, M. (eds.) *Policing Across National Boundaries*. London, Pinter, pp. 161–173.
- Bigo, D. (1998) Sécurité et immigration: vers une gouvernementalité par l'inquiétude?. *Cultures et Conflits*. 31–32: 13–38.
- Bigo, D. (2002) Security and immigration: Toward a critique of the governmentality of unease. *Alternatives: Global, Local, Political*. 27(1): 63–92.
- Bourdieu, P. (1993) *The Field of Cultural Production*. Cambridge, Polity Press.
- Buzan, B. & Wæver O. (2003) *Regions and Powers*. Cambridge, Cambridge University Press.
- Buzan, B. (2004) *The United States and the Great Powers: World Politics in the Twenty-First Century*. Cambridge, Polity.
- Buzan, B., Wæver O., & de Wilde, J. (1998) *Security: A New Framework for Analysis*. Boulder, Lynne Rienner.
- c.a.s.e. collective (2006). Critical approaches to security in Europe: A networked manifesto. *Security Dialogue*. 37(4): 443–487.
- Clarke, R. & Knake, R. (2012) Cyber war: The next threat to national security and what to do about it. *Strategic Analysis*. 39(4): 458–460.
- Clinton, W.J. (2000) *Defending America's Cyberspace: National Plan for Information Systems Protection. An Invitation to a Dialogue. Version 1.0*. Washington, DC: US Government Printing Office.
- Collier, J. (2018) Cybersecurity assemblages: A framework for understanding the dynamic and contested nature of security provision. *Politics and Governance*. 6(2): 13–21.
- Drucker, P.F. (1989) *The New Realities: In Government and Politics, in Economics and Business, in Society and World View*. New York, Harper Collins Publishers.
- Dunn Cavelt, M. (2008) *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London, Routledge.
- Dunn Cavelt, M. (2012) The militarisation of cyber security as a source of global tension. In Möckli, D. & Wenger, A. (eds.) *Strategic Trends Analysis 2012*. Zurich, Center for Security Studies.

- Dunn Cavelty, M. & Suter, M. (2012) The art of CIIP strategy: Taking stock of content and processes. In Lopez, J., Setola, R., & Wolthusen S.D. (ed.) *Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense*. Springer, pp. 15–38.
- Edwards, P.N. (1996) *The Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge, MIT Press.
- Eriksson, J. (2001) Cyberplagues, IT, and security: Threat politics in the information age. *Journal of Contingencies and Crisis Management*. 9(4): 211–222.
- Eriksson, J. & Giacomello, G. (2006) The information revolution, security, and international relations: (IR)relevant theory? *International Political Science Review*. 27(3): 221–244.
- Haacke, J. & Williams, P.D. (2008) Regional arrangements, securitization, and transnational security challenges: the African Union and the Association of Southeast Asian Nations compared. *Security Studies*. 17(4): 775–809.
- Hagmann, J. & Dunn Cavelty, M. (2012) National risk registers: Security scientism and the propagation of permanent insecurity. *Security Dialogue*. 43(1): 80–97.
- Hansen, L. (2006) *Security as Practice. Discourse Analysis and the Bosnian War*. London, Routledge.
- Hansen, L. (2012) Reconstructing desecuritisation: The normative-political in the Copenhagen School and directions for how to apply it. *Review of International Studies*. 38(3): 525–546.
- Hansen, L. & Nissenbaum, H. (2009) Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*. 53(4): 1155–1175.
- Huysmans, J. (1998) The Question of the limit: Desecuritisation and the aesthetics of horror in political realism. *Millennium – Journal of International Studies*. 27(3): 569–589.
- Huysmans, J. (2006) *The Politics of Insecurity: Fear, Migration and Asylum in the EU*. London, Routledge.
- Huysmans, J. (2008) The jargon of exception – on Schmitt, Agamben and the absence of political society. *International Political Sociology*. 2(2): 165–183.
- Huysmans, J. (2011) What's in an Act? On security speech acts and little security nothings. *Security Dialogue*. 42(4–5): 371–383.
- Lawson, S. (2013) Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyberthreats. *Journal of Information Technology & Politics*. 10(1): 86–103.
- Léonard, S. (2010) EU border security and migration into the European Union: FRONTEX and securitization through practices. *European Security*. 19(3): 231–254.
- Léonard, S. & Kaunert C. (2011) Reconceptualizing the audience in securitization theory. In Balzacq, T. (ed.) *Securitization Theory: How Security Problems Emerge and Dissolve*. London, Routledge, pp. 57–76.
- Lobo-Guerrero, L. (2008) 'Pirates', stewards, and the securitization of global circulation. *International Political Sociology*. 2: 219–235.
- McDonald, M. (2008) Securitization and the construction of security. *European Journal of International Relations*. 14 (4): 563–587.
- Mutimer, D., Grayson, K., & Marshall Beier J. (2013) Critical studies on security: An introduction. *Critical Studies on Security*. 1(1): 1–12.
- Rona, T.P. (1976) *Weapon Systems and Information War*. Boeing Aerospace Co. Research Report, Seattle: Boeing.
- Salter, M.B. (2008) Securitization and desecuritization: A dramaturgical analysis of the Canadian Air Transport Security Authority. *Journal of International Relations and Development*. 11(4): 321–349.
- Searle, J.R. (1969) *Speech Acts: An Essay in the Philosophy of Language*. Cambridge, Cambridge University Press.
- Shires, J. (2018) Enacting expertise: Ritual and risk in cybersecurity. *Politics and Governance*. 6(2): 31–40.
- Stevens, T. (2016) *Cybersecurity and the Politics of Time*. Cambridge, Cambridge University Press.
- Stevens, T. (2018) Cyberweapons: Power and the governance of the invisible. *International Politics*. 55(3–4): 482–502.
- Stritzel, H. (2007) Towards a theory of securitization: Copenhagen and beyond. *European Journal of International Relations*. 13(3): 357–383.
- Toffler, A. (1981) *Power Shift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*. New York, Bantam Books.
- Vuori, J.A. (2008) Illucutionary logic and strands of securitization: Applying the theory of securitization to the study of non-democratic political orders. *European Journal of International Relations*. 14(1): 65–99.

- Wæver, O. (1995) Securitization and desecuritization. In Lipschutz, R.D. (ed.) *On Security*. New York/Chichester, Columbia University Press, pp. 46–86.
- Wæver, O. & Buzan, B. (2015) After the return to theory: The past, present, and future of security studies. In Collins, A. (ed.) *Contemporary Security Studies*, 4th edition. Oxford, Oxford University Press, pp. 417–435.
- Walt, S.M. (1991) The Renaissance of Security Studies. *International Studies Quarterly*. 35(2): 211–239.

2

CORRELATES OF STATE-SPONSORED CYBER CONFLICT

George E. Mitchell and Allison Pytlak

State-to-state engagement in cyberspace is a rapidly developing reality of contemporary international relations (Farwell and Rohozinski, 2012). Policymakers, scholars, and pundits alike express alarmism over the destructive potential of cyber conflict, often likening the severity of the threat to the specter of nuclear warfare. But what do we really know about state to state cyber conflict empirically? Despite growing fears, relatively little empirical research exists systematically examining patterns of cyber conflict. To address this research gap, this article examines historical patterns of publicly known state-sponsored cyberattacks among rival state dyads from 2000 to 2014 to identify the correlates of cyber conflict and to consider their theoretical implications.

This chapter is organized as follows: the next section briefly reviews prior literature pertaining to state to state cyber conflict, characterizing its evolution as a dialectical process. The subsequent section identifies specific hypotheses about the strategic logic of cyber conflict that have emerged from this literature, observing many contradictory propositions. This section is followed by a more precise statement of empirical expectations. The sections after that introduce the data and method and then report and interpret the results of the analysis. The chapter ends with a brief conclusion summarizing major findings, reiterating important limitations, and providing suggestions for future research.

The dialectics of cybersecurity discourse

The literature on cyber conflict reflects a dialectical process of thesis and antithesis, presenting many contradictory positions on the basic principles of cyber conflict and struggling to move toward synthesis (e.g. Lindsay and Kello, 2014). Langø (2016) observes two established and one emerging school of thought in this regard. Cyber-alarmists view cyber conflict as an important new domain of military power that threatens to upend traditional understandings of conflict and frequently warn of digital Pearl Harbors and 9/11s in which the technological vulnerabilities of complacent states invite cyber devastation (e.g. Clarke and Knake, 2012; Arquilla and Ronfeldt, 1993). Cyber-moderates, on the other hand, view the cyber domain as an auxiliary domain of conflict at best, with little strategic value in isolation from kinetic conflict. Cyber-moderates point to the empirical rarity of cyber conflict and its generally low-level nature to argue against cyber-alarmism

(Valeriano and Maness, 2014; Gartzke and Lindsay, 2015; Dipert, 2010; Lindsay, 2013, Rid, 2013b; Gartzke, 2013).

Meanwhile, an emerging group of cyber-comparativists seek mainly to understand the logic of cyber conflict, often through comparisons or analogies with other forms of power, such as land, sea, air, and nuclear (Langø, 2016; Libicki, 2009; Rattray, 2001, 2009). Although scholars and policymakers continue to debate the severity of the threat of cyber conflict, few would deny its potential to cause harm and so generally agree that continued theoretical and empirical inquiry is warranted (Arquilla, 2012).

Inquiry into the nature of the cyber threat is complicated by an elaborately contested discourse. Cyber-alarmists, conceiving of cyber conflict as an evolutionary development in the waging of conventional warfare (Limnell, 2014), adopt terms such as ‘cyberwar’ and ‘cyberattack’. However, cyber-moderates argue that cyber conflict generally does not rise to the level of warfare and so militaristic discourse is misleading. According to Rid (2013a; 2012), for example, warfare is violent, instrumental, and political, whereas most cyber conflict typically only consists of subversion, espionage, or sabotage.

Many critical scholars have examined the evolution of cyber security discourse (Manjikian, 2010, Hansen and Nissenbaum, 2009) and have expressed concerns over its conceptual transition “from a ‘geekspace’ into a ‘battlespace’” (Hughes 2010, p. 524), as well as its ‘securitization’ and ‘militarization’—whereas cyberspace could otherwise be regarded as a domain of civil society (Deibert, 2003), for example. They note that cyber discourse is dominated by references to the surprise attacks of Pearl Harbor and 9/11, and to enduring strategic conflicts such as the Cold War, all of which frame cyber security as a military issue (Dunn Cavelt, 2013). Threat inflation, a war framing, and a preoccupation with doomsday scenarios are seen as rampant and unhelpful, and may be counterproductive (Lawson, 2013; Brito and Watkins, 2011).

Framing the cyber debate are fundamentally conflicting interpretations of cyberspace. For cyber-alarmists, cyberspace represents a new and uncertain domain of military warfare that threatens the status quo through an unpredictable redistribution of capabilities and vulnerabilities. For cyber-moderates, the threat of cyber conflict is both more limited and more predictable. Meanwhile, discursive (or perhaps ontological) confusion persists as to whether cyber conflict is a proper domain of interstate warfare, as even those attempting to articulate a synthetic position appear to concede a militaristic framing of the issue. Consistent with the contested discourse and its dialectic of alarmism, moderatism, and comparitivism, cyber conflict theory itself exhibits similar disparities and contradictions.

Cybersecurity’s contradictions

As the dialectical and contested framing of the cyber debate suggests, the literature specifically concerning the strategic logic of state-sponsored cyber conflict provides a tangle of contradictory hypotheses and counter-hypotheses. However, while scholars may disagree about *how* certain characteristics matter, broad agreement appears to exist about *whether* certain characteristics matter. These characteristics include 1) states’ degrees of absolute and relative power, 2) their capabilities and vulnerabilities, and 3) the prospects for deterrence and retaliation, among others.

Among the most persistent and frequently debated speculations about cyber conflict is the specter of an asymmetric surprise attack perpetrated by a weaker state against a stronger state—akin to the so-called ‘digital Pearl Harbor’ or ‘digital 9/11’ scenarios (Lynn III, 2010). Under this view asymmetries in vulnerabilities between weaker and stronger states

give weaker states the advantage (Nye, 2010). Smaller, militarily weaker, less economically developed states are less vulnerable, while their larger, militarily stronger, more economically developed rivals are more vulnerable. This inversion creates a leveling effect that encourages weaker states to initiate cyber conflict against their more conventionally powerful foes. This advantage is made possible by the relatively low barrier to entry for weaker states to obtain cyber weapons, particularly in comparison to other strategic capabilities, such as nuclear weapons. In short, the more advanced and powerful the state the greater its reliance on cyber systems and therefore the more vulnerable it is to an attack (Nye, 2010; Lindsay, 2013; Adams, 2001).

One consequence of these assumptions is the view that cyber conflict favors the offense (Kello, 2013; Arquilla, 2012). Cyber defense will always lag behind cyber offense, as critical vulnerabilities only become apparent in the aftermath of an attack (Lynn III, 2010). However, skeptics point out that if the cyber domain is genuinely offense-dominant, and if cyber capabilities are within the means of even weak actors, then cyber conflict should be much more frequent and severe than it has been historically (Gartzke and Lindsay, 2015). Indeed, empirical research examining the historical frequency and intensity of cyber conflict observes the puzzling phenomenon of ‘cyber restraint,’ contrary to the predictions of cyber-alarmists (Valeriano and Maness, 2014). Deterrence and fear of retaliation and escalation may explain why cyber conflict is rare among rivals and why low-level operations appear to be tolerated (Valeriano and Maness 2014, pp. 349–351) or it may be that high-level cyber operations are rare simply because they are more difficult to conduct (Lindsay, 2013). Additionally, cyber restraint may prevail because although weak actors are said to be able to develop cyber weapons in principle, evidence indicates that in practice they lack of the requisite technological sophistication and conventional follow-through capabilities (Liff 2012, p. 417). Under this alternative view, cyber conflict requires a sophisticated state aggressor (Rid, 2012) and is therefore most likely to be initiated by a larger, more powerful state that has already achieved sufficient conventional as well as cyber capabilities.

Many others join this challenge to the asymmetric threat hypothesis to argue that the cyber domain instead simply reflects the status quo distribution of power. “Cyberpower rewards already powerful states with even more capability,” according to Betz (2012, p. 695). Gartzke and Lindsay (2015, p. 345) argue that powerful states have this advantage

because intelligence is costly and its exploitation is complicated, [and] wealthier and larger states tend to have more sophisticated, robust intelligence capacities. Only capable actors, such as major powers, are likely to be able to master the complex tango of deception and counter-deception necessary to execute high-intensity operations.

The questions as to whether the cyber domain is offense or defense dominant, and whether it favors weak or strong actors, may also be tied to the problem of attribution in cyber conflict. No one seriously debates whether it was Japan that bombed Pearl Harbor or Al Qaeda that perpetrated the 9/11 attacks, yet cyber skirmishes are often shrouded in secrecy and seldom attributed without controversy. Anonymity may play to the advantage of the attacker if they are able to influence the victim without risk of retaliation. The ability to execute a significant cyber-attack undetected requires a technologically sophisticated state with the capacity not only to successfully deliver the blow but also to conceal its identity. The attribution issue may therefore reverse the logic of asymmetric warfare alarmism in several ways (Rid and Buchanan, 2015). First, it is strong states, not weak states that have the most sophisticated cyber capabilities and that will therefore be the most likely to initiate cyber conflict,

particularly if they believe they can do so covertly. Second, strong states are the least likely to be the target of cyber-attacks because they also have the greatest abilities to detect and retaliate against would-be aggressors. Anticipating this in advance, potential instigators of asymmetric conflict would exercise restraint. Again, this goes against the views of other scholars who posit that strong states are particularly vulnerable, underlining the contradictions that pervade cyber conflict theory.

The risks of retaliation and escalation raise the issue of cyber deterrence, particularly involving weaker powers seeking to harm conventionally more powerful adversaries. The logic of deterrence turns out to be a difficult concept to graft on to the cyber domain, however, and many authors argue that conventional theories of deterrence do not readily apply to cyber conflict (Nye, 2010; Libicki, 2009; Lupovici, 2011). According to Libicki (2009), the threat of cyber retaliation is not credible because the retaliator cannot count on disarming its adversary's cyber capabilities. Moreover, simply announcing a credible cyber threat both eliminates deniability and ensures that the adversary will adopt defensive preventive measures. Even a preemptive attack or compellance strategy is ineffective because destroying the adversary's cyber offenses cannot be guaranteed. Liff (2012, p. 419) poses the difficulty this way:

There are several reasons why such deterrence efforts will probably be ineffective. First is the stability-instability paradox, which suggests that while nuclear- or conventional-based deterrence may be sufficient to sharply reduce the probability of a direct nuclear or conventional exchange between two or more actors, it may simultaneously increase the probability of a minor conflict between them at a lower level of conflict; in this case, in the cyber-domain. Seeking to avoid potentially catastrophic nuclear or conventional war and assuming that neither side will allow a cyber exchange to escalate, a potential aggressor may be more willing to use [cyber conflict] in order to coerce its adversary, particularly when its strategic objectives are limited.

In this logic of cross-domain deterrence the retaliatory capabilities attendant to nuclear weapons possession are not a credible deterrent to cyber conflict because adversaries know that they are mutually unwilling to escalate a cyber dispute to conventional or nuclear war. Consistent with Liff's expectations, prior empirical research has found that nuclear weapons possession is indeed associated with an increased likelihood of cyber conflict (Pytlak and Mitchell, 2016), further suggesting that escalatory cross-domain deterrence is ineffective. Due to the unwillingness of states to undertake cyber operations that risk escalation to the conventional or nuclear domains, persistent cyber skirmishes among powerful states involving low-level probes and incursions calculated to avoid escalation are a much more likely scenario than all-out cyber Armageddon (Dipert, 2010).

High-level, highly destructive cyber-attacks are also extremely difficult to reliably execute—even for powerful states (Lindsay, 2013) and they carry a highly uncertain probability of success (Gartzke and Lindsay, 2015). Although many concede that catastrophic escalation is nevertheless possible (Betz, 2012; Gompert and Libicki, 2015), so far there is very little evidence of spillover from the cyber domain to the kinetic domain (Maness and Valeriano, 2016). Within-domain retaliation may be more likely, with prior victimization a likely predictor of 'reciprocal' cyber action.

Finally, if comparativist analogies to traditional conflict domains are appropriate, then additional factors posited to affect the likelihood of conventional interstate conflict generally, such as trade interdependence and political openness, (Oneal and Russett, 1999; Gartzke and

Li, 2003; Russett and O’Neal, 2000; Hegre, 2014; Hegre, Oneal, and Russett, 2010), may similarly affect the likelihood of conflict in the cyber domain. Important differences exist between cyber conflict and kinetic warfare that may imperil analogies between these two domains. Most importantly, cyber conflict has generally been limited to relatively low-level intrusions whose purposes fall well short of traditional war aims (Jensen, Valeriano, and Maness, 2016).

Although less commonly studied within cybersecurity literature, prior research suggests that it may be reasonable to speculate that cyber conflict is conditioned by similar factors as traditional conflict.

Empirical expectations

Prior research has called for more theoretical (Junio, 2013) as well as empirical research into the logic and correlates of state-sponsored cyber conflict, particularly research that moves beyond single-case inferences to test hypotheses using datasets “drawing on the variety of known cases” of cyber conflict worldwide (Kello 2013, p. 15). Although obvious difficulties abound in large- n cyber conflict research, the persistence of so many contradictory theoretical claims clearly warrants further investigation.

Although cyber conflict theory is ambiguous about *how* specific characteristics matter for conditioning cyber conflict, it is somewhat clearer about *which* characteristics should matter. Specifically, the likelihood of state-sponsored cyber conflict may depend upon: (H1) prior victimization (indicative of within-domain retaliation), (H2) nuclear weapons possession, (H3) dyadic asymmetry, (H4) the absolute size or power of the initiator, (H5) the absolute size or power of the target, (H6) the initiating state’s reliance on technology, (H7) the target state’s reliance on technology – and drawing from comparativism – (H8) the political openness of the initiator, (H9) the political openness of the target, (H10) the trade dependence of the initiator on the target, and (H11) the trade dependence of the target on the initiator. In accordance with theoretical expectations, we test *whether* ($H : \beta \neq 0$) rather than *how* ($H : \beta \leq 0$) these factors matter.

Data and method

Cyber conflict data are obtained from the Cyber Conflict Dataset version 1.5 by Valeriano and Maness (2015; 2014). This dataset contains information on dyads of rival states extracted from Thompson’s (2001) strategic rivalry dataset and Klein et al.’s (2006) enduring rivalry dataset, focusing specifically on rivals due to their greater likelihood of conflict (Valeriano and Maness, 2014, p. 347). The rivalry dataset (Klein, Goertz, and Diehl, 2006) is an extension of the Correlates of War project (Palmer et al., 2015; Ghosn, Palmer, and Bremer, 2004). The Cyber Conflict Dataset includes four dyads subsequently added to the rivalry dataset: Iran–Saudi Arabia, Syria–Israel, Russia–Estonia and China–India.

Valeriano and Maness regard rivalries as ‘possessing and varying across four constituent dimensions: 1) spatial consistency, 2) duration, 3) militarized competitiveness, and 4) linked conflict’. They (2014, pp. 348, 350) adopt a general definition of rivalry as a ‘longstanding conflict with a persistent enemy’ and define cyber conflict as ‘the use of computational technologies in cyberspace for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities short of war and away from the battlefield’. Their dataset contains 165 cyber incidents nested within 51 cyber disputes over the period 2000–2014 (Maness and Valeriano, 2015) and claims to represent ‘all publicly acknowledged

cyber incidents and disputes between rival states' where cyber incidents are 'individual operations launched against a state' and 'cyber disputes are specific campaigns between two states using cyber tactics during a particular time period and can contain one to several incidents, often including an initial engagement and responses' (Valeriano and Maness, 2014, pp. 349, 355).

While not without controversy (Valeriano et al., 2016), we regard Valeriano and Maness's codings and attributions as representing the best available dataset on publicly known state-sponsored cyber conflict currently available. In addition to their dataset, we also rely on several other data sources to provide information for 198 directed state dyads for the 15-year period from 2000–2014, yielding a total sample size of 2,970 directed dyad-years. The pertinent variables and their respective data sources are described below.

Cyber conflict initiation. The dependent variable is a dichotomous measure of cyber conflict initiation by directed dyad-year (A→B) adapted from the Cyber Conflict Dataset version 1.5 (Maness and Valeriano, 2015). Our dataset contains 145 instances of cyber conflict initiation within 36 of 198 directed dyads over the fifteen-year period. For clarity and concision, we denote the real or potential initiator as state 'A' and the real or potential target as state 'B'.

Prior victimization. A prior target of B is a dichotomous variable indicating whether the cyber conflict initiator was previously targeted by its rival in any prior year within the panel. Data are adapted from the Cyber Conflict Dataset version 1.5 (Maness and Valeriano, 2015).

Nuclear weapons possession. Nuclear weapons possession is a nominal variable identifying the pattern of bilateral nuclear weapons possession within each directed dyad. Its values include neither, B only, A only, and both, with neither serving as the reference category. Data are obtained from the Federation of American Scientists.

Dyadic asymmetry. Four variables are considered. Military advantage of A is a ratio variable measuring the difference in total annual military expenditures between state A and state B relative to their combined total annual military expenditures. Data are sourced from the Stockholm International Peace Research Institute Military Expenditure Database. Economic advantage of A is a ratio variable measuring the difference in GDP per capita between state A and state B relative to their combined GDP per capita. Data are sourced from the UN and the World Bank. Population advantage of A is a ratio variable measuring the difference in population between state A and state B relative to their combined population. Data are sourced from the World Bank. Overall advantage of A is a factor derived from military advantage, economic advantage, and population advantage, derived from principal component factor analysis. The solution yields a single dominant factor with an Eigenvalue of 2.57 and an alpha reliability of 0.91. The factor is similar to the mean of the three constituent variables.

Absolute size and power (initiator and target). This is proxied by GDP. GDP data are sourced from the UN and the World Bank, and are measured in current \$US billions.

State's reliance on technology (initiator and target). This is proxied by internet penetration, which measures the percentage of the population who have accessed the internet within the preceding year. Data are sourced from the World Bank and internetlivestats.com.

Political openness (initiator and target). Voice and accountability scores measure political openness, or more specifically, perceptions of political participation, freedom of expression, freedom of association, and media freedom. Scores logically range from -2.5 (weak) to 2.5 (strong). Data are obtained from the World Bank's Worldwide Governance Indicators Project.

Trade dependence (initiator and target). Trade dependence of A on B and Trade dependence of B on A are ratio variables measuring a state's imports from its rival as a percentage of its GDP. Data are sourced from the International Monetary Fund's Direction of Trade statistics and the Organization for Economic Cooperation and Development Structural Analysis Bilateral Trade Database.

Year. Year indicates the calendar year and is included as a control variable.

Regression results are obtained from two rounds of data analysis. First, population-averaged generalized estimating equations using robust standard errors provide estimates of effects for the average directed dyad. Second, fixed effects models provide estimates for time-variant characteristics (excluding nuclear weapons possession) within the subset of cyber-active dyads. Unlagged and lagged models are presented to assess time lag effects. Alternative models are estimated substituting overall advantage for military advantage, economic advantage, and population advantage because the three related variables are highly correlated. Missing data are handled with listwise deletion (Allison 2001); data missingness is statistically independent of both dyadic cyber conflict activity ($p = 0.86$, $n = 2970$) and cyber conflict initiation ($p = 0.65$, $n = 2970$).

Results

Table 2.1 summarizes the hypotheses and results. Table 2.2 presents the results of four population-averaged models (which represent effects for the ‘average’ dyad). The first set of models demonstrates that four characteristics are consistently associated with a higher propensity for cyber conflict initiation: prior victimization, bilateral nuclear weapons possession, the size of the target state’s economy, and low levels of voice and accountability.

Table 2.1 Hypotheses and results

<i>Hypothesis ($H : \beta \neq 0$)</i>	<i>Result</i>
H1: Prior victimization	Partial support; Prior targets more likely to initiate an attack (Table 2.2)
H2: Nuclear weapons possession	Support; Bilateral nuclear weapons possession associated with increased likelihood of conflict (Table 2.2)
H3: Dyadic asymmetry in state capabilities and vulnerabilities	Weak to no support; Only prior economic advantage of the initiator is associated with an increased likelihood of conflict (Table 2.3)
H4: Absolute state size, power, or sophistication of initiator	Partial support; Larger states less likely to initiate (Table 2.3)
H5: Absolute state size, power, or sophistication of target	Strong support; Larger states more likely to be targets (Tables 2.2 and 2.3)
H6: Initiating states’ reliance on technology	No support
H7: Target state’s reliance on technology	Partial support; Less technologically reliant states less likely to be targets (Table 2.3)
H8: Political openness of initiator	Strong support; More open states less likely to initiate (Tables 2.2 and 2.3)
H9: Political openness of target	Partial support; More open states less likely to be targets in subsequent year (Table 2.3)
H10: Trade dependence of initiator	No support
H11: Trade dependence of target	Weak support; Prior dependence of target on initiator associated with increased likelihood of attack (Table 2.3)

Table 2.2 Population averaged models for cyber conflict initiation

	Model 1		Model 2 (Lagged)		Model 3		Model 4 (Lagged)	
	Coef.	S.e.	Coef.	S.e.	Coef.	S.e.	Coef.	S.e.
A prior target of B								
No								
Yes	1.10	0.52 **	0.96	0.52 *	1.13	0.55 **	0.95	0.54 *
Nuclear weapons possession								
Neither								
B only	-0.40	1.84	-0.67	1.94	-1.25	1.68	-1.15	1.83
A only	2.04	1.43	2.29	1.43	2.29	1.43	2.45	1.41 *
Both	2.89	1.25 **	3.12	1.20 ***	2.69	1.17 **	3.02	1.19 **
Military advantage of A	1.09	1.16	0.63	1.31				
Economic advantage of A	-1.25	1.12	-0.68	1.15				
Population advantage of A	0.15	0.80	0.12	0.83				
Overall advantage of A					-0.20	0.63	-0.07	0.62
GDP A ^a	0.10	0.07	0.08	0.07	0.10	0.06	0.09	0.07
GDP B ^a	0.19	0.09 **	0.23	0.10 **	0.21	0.10 **	0.24	0.11 **
Internet penetration A	1.27	1.54	1.37	1.29	1.27	1.53	1.34	1.29
Internet penetration B	0.23	1.40	-0.39	1.31	0.36	1.22	-0.28	1.17
Voice and Accountability A	-0.78	0.36 **	-0.80	0.35 **	-0.80	0.35 **	-0.82	0.34 **
Voice and Accountability B	-0.17	0.44	-0.10	0.46	-0.12	0.44	-0.09	0.47
Trade dependence A on B	-5.47	8.60	0.00	7.59	-3.53	8.56	0.81	7.89
Trade dependence B on A	-0.43	4.67	-1.51	4.88	-1.26	4.70	-2.02	4.78
Year	0.03	0.05	0.03	0.05	0.02	0.05	0.03	0.05
Constant	-61.64	102.64	-68.28	102.77	-47.55	98.06	-60.41	98.42
Observations	2122		1968		2122		1968	
Groups	170		170		170		170	
χ^2	104.64	***	77.36	***	102.89	***	76.83	***

a Statistics multiplied by 1,000 for convenience of display.

The results of Model 1 illustrate the general findings. While the overall prevalence of cyber conflict is low, the predicted probability of cyber conflict is significantly higher when a state has previously been targeted by its rival. The predicted probability of cyber conflict initiation increases from 0.04 to 0.09. Bilateral nuclear weapons possession more dramatically increases the probability of cyber conflict initiation. The predicted probability increases from 0.02 if neither state possesses nuclear weapons to 0.16 when both states possess nuclear weapons.

The results also reveal that cyber conflict initiation is more likely when the target state's economy is large, however, the effect is substantively negligible for all but the largest economies in the world, such as the US and China. Figure 2.1 displays the probability of cyber conflict initiation as a function of the target state's GDP.

Finally, states with higher levels of political openness are less likely to initiate cyber conflict. Figure 2.2 displays the predicted probability of cyber conflict initiation as a function of state A's voice and accountability score.

Neither relative advantages, the size of the initiator's economy, internet penetration, the target state's level of voice and accountability, nor trade dependence exhibited statistically significant effects in the population-averaged models. The control variable for the calendar year is also insignificant. Finally, variation in time lag does not appear to introduce substantial differences in effect magnitudes or significance levels.

Table 2.3 presents the results of the fixed effects regressions for the subset of cyber-active dyads (which represent 'within-dyad' effects). As before, states with larger economies are consistently more likely to become targets of cyber conflict, while states with more political openness are consistently less likely to initiate cyber conflict. Additional results emerge here as well. Findings indicate that states with larger economies are less likely to initiate cyber conflict. Moreover, states with higher levels of internet penetration and political openness in prior years are less likely to be targeted.

Figure 2.1 Probability of cyber conflict initiation as a function of state B's GDP (Model 1)

Figure 2.2 Probability of cyber conflict initiation as a function of state A's voice and accountability score (Model 1)

Table 2.3 Fixed effects models for cyber conflict initiation

	<i>Model 1</i>		<i>Model 2 (Lagged)</i>		<i>Model 3</i>		<i>Model 4 (Lagged)</i>	
	<i>Coef.</i>	<i>S.e.</i>	<i>Coef.</i>	<i>S.e.</i>	<i>Coef.</i>	<i>S.e.</i>	<i>Coef.</i>	<i>S.e.</i>
A prior target of B								
No								
Yes	-0.86	0.62	-0.81	0.68	-0.77	0.61	-0.92	0.65
Military advantage of A	0.51	4.12	-5.01	4.52				
Economic advantage of A	-0.16	3.84	9.59	4.26				
Population advantage of A	35.22	22.12	40.82	22.19				
Overall advantage of A					0.78	2.33	5.06	2.42
GDP A ^a	-0.38	0.19	-0.65	0.22	-0.42	0.19	-0.06	0.02
GDP B ^a	1.21	0.49	1.83	0.65	1.29	0.48	0.17	0.06
Internet penetration A	-1.65	2.10	-1.30	2.28	-2.30	2.07	-1.81	2.25
Internet penetration B	-4.68	2.44	-7.68	2.68	-3.89	2.33	-6.06	2.46

(Continued)

	<i>Model 1</i>		<i>Model 2 (Lagged)</i>		<i>Model 3</i>		<i>Model 4 (Lagged)</i>	
	<i>Coef.</i>	<i>S.e.</i>	<i>Coef.</i>	<i>S.e.</i>	<i>Coef.</i>	<i>S.e.</i>	<i>Coef.</i>	<i>S.e.</i>
Voice and Accountability A	-6.48	2.03 ***	-5.53	1.69 ***	-5.72	1.87 ***	-4.37	1.44 ***
Voice and Accountability B	-2.32	1.79	-4.74	1.59 ***	-2.84	1.76	-5.15	1.48 ***
Trade dependence A on B	-52.00	59.62	57.89	48.79	-60.66	54.57	26.72	44.54
Trade dependence B on A	19.85	15.63	33.99	16.87 **	20.99	15.18	29.98	16.35 *
Year	0.41	0.12 ***	0.43	0.13 ***	0.39	0.12 ***	0.41	0.13 ***
Observations	370		331		370		331	
Groups	25		24		25		24	
χ^2	87.94	***	84.55	***	85.41	***	79.38	***

a Statistics multiplied by 1,000 for convenience of display.

Conclusions and implications

These results help to advance our understanding of state-sponsored cyber conflict. Three findings stand out. First, bilateral nuclear weapons possession is associated with an increased likelihood of cyber conflict, lending credibility to the stability-instability paradox in the cyber domain, in which the specter of catastrophic escalation may increase the likelihood of lower level conflict. Second, larger states are more likely to be targets of cyber conflict, regardless of dyadic asymmetry. This is consistent with the vulnerability hypothesis, which posits that that larger states present more targets of opportunity. Third, more politically open states appear to be less likely to initiate cyber conflict, suggesting that certain ‘liberal peace’ style dynamics thought to condition traditional interstate conflict may also apply to the cyber domain. A variety of other specific findings also obtain but lack commensurately robust support.

A number of important limitations to this study warrant caution in interpreting and extrapolating its findings. First, the instances of cyber conflict contained in the underlying dataset mainly consist of relatively low-level cyber activity evidently taking place within a ‘zone of tolerance’. Massively disruptive, large-scale cyber operations may be more likely to invite cross-domain retaliation and alter the logic and practice of cyber conflict. Second, historical patterns of state-sponsored cyber conflict may turn out to be a poor guide to the future, particularly in the dynamic cyber domain where sudden innovations in technology could rapidly alter distributions of offensive and defensive capabilities. Third, the analysis is limited to publicly known instances of cyber conflict, and only among rival dyads, which excludes a much larger pool of presumably lower-level, still-clandestine cyber operations involving non-rivals. Fourth, attribution in cyber conflict is often subject to dispute, particularly when states have motivations for deception. Finally, the analysis excludes cyber operations taking place exclusively among nonstate actors, which are growing in frequency and significance and therefore deserving of systematic research. Readers should carefully consider these important limitations.

Future scholarship would do well to continue to critically scrutinize and improve upon existing data sources pertaining to state-sponsored cyber conflict. In addition to the need for more and better data, more interaction between theoretical development and empirical evidence is also needed. Theoretical conjecture often far outpaces empirical research about cyber conflict, which can obfuscate both scholarship and policy making with contradictory postulations of seemingly equal plausibility. As emerging norms continue to develop around cybersecurity and its study and conceptualization, concerns have been expressed about threat inflation and the rapid militarization of cyberspace. More frequent and systematic empirical research can help to ensure that cybersecurity discourse remains grounded.

References

- Adams, J. (2001) Virtual defense. *Foreign Affairs*. 80(3).
- Allison, P.D. (2001) *Missing Data*. Sage University Papers Series on Quantitative Applications in the Social Sciences, 07–136. Thousand Oaks, Sage.
- Arquilla, J. (2012) Cyberwar is already upon us. *Foreign Policy*. 192(March/April): 1–4.
- Arquilla, J. and Ronfeldt D. (1993) Cyberwar is Coming! *Comparative Strategy*. 12 (2):141–165.
- Asal, V., Mauslein, V., Murdie, A., Young, J., Cousins, K., and Bronk, C. (2016) Repression, education, and politically motivated cyberattacks. *Journal of Global Security Studies*. 1(3): 234–246.
- Betz, D. (2012) Cyberpower in strategic affairs: Neither unthinkable nor blessed. *Journal of Strategic Studies*. 35(5): 689–711. doi: 10.1080/01402390.2012.706970.
- Brito, J. and Watkins, T. (2011) Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. *National Security Journal*. 3(1): 39–84.
- Clarke, R.A. and Knake, R.K. (2012) *Cyber War: The Next Threat to National Security*. New York: Harper Collins.
- Colaresi, M.P., Rasler, K., and Thompson, W.R. (2007) *Strategic Rivalries in World Politics: Position, Space and Conflict Escalation*. Cambridge, Cambridge University Press.
- Deibert, R.J. (2003) Black code: Censorship, surveillance, and the militarisation of cyberspace. *Milennium*. 32(3): 501–530.
- Dipert, R.R. (2010) The ethics of cyberwarfare. *Journal of Military Ethics*. 9(4): 384–410. doi: 10.1080/15027570.2010.536404.
- Dunn Cavelt, M. (2013) From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*. 15: 105–122.
- Farwell, J.P. and Rohozinski, R. (2012) The new reality of cyber war. *Survival*. 54(4): 107–120. doi: 10.1080/00396338.2012.709391.
- Gartzke, E. (2013) The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security*. 38(2): 41–73.
- Gartzke, E. and Li, Q. (2003) Measure for measure: Concept operationalization and the trade interdependence-conflict debate. *Journal of Peace Research*. 40: 553–571.
- Gartzke, E. and Lindsay, J.R. (2015) Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*. 24: 316–348.
- Ghosn, F., Palmer, G., and Bremer, S.A. (2004) The MID3 Data Set, 1993–2001: Procedures, coding rules, and descriptions. *Conflict Management and Peace Science*. 21(2): 133–154.
- Goertz, G. and Diehl, P.F. (2001) *War and Peace in International Rivalry*. Ann Arbor, University of Michigan Press.
- Gompert, D.C. and Libicki, M. (2015) Waging cyber war the American way. *Survival*. 57(4): 7–28. doi: 10.1080/00396338.2015.1068551.
- Hansen, L. and Nissenbaum, H. (2009) Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*. 53: 1155–1175.
- Hegre, H. (2014) Democracy and armed conflict. *Journal of Peace Research*. 51(2): 159–172.
- Hegre, H., Oneal, J.R., and Russett, B. (2010) Trade does promote peace: New simultaneous estimates of the reciprocal effects of trade and conflict. *Journal of Peace Research*. 47(6): 763–774.
- Hughes, R. (2010) A Treaty for Cyberspace. *International Affairs*. 86(2): 523–541.

- Jensen, B.M., Valeriano, B., and Maness, R.C. (2016). *The Efficacy of Cyber Coercion: Compellence in the Digital Domain*.
- Junio, T.J. (2013) How Probable is cyber war? Bringing IR theory back in to the cyber conflict debate. *Journal of Strategic Studies*. 1–9. doi: 10.1080/01402390.2012.739561
- Kello, L. (2013) The meaning of the cyber revolution: perils to theory and statecraft. *International Security*. 38(2): 7–40.
- Klein, J.P., Goertz, G., and Diehl, P.F. (2006) The new rivalry dataset: Procedures and patterns. *Journal of Peace Research*. 43(3): 331–348.
- Langø, H-I. (2016) Competing academic approaches to cyber security. In Friis, K. and Ringsmose, J. (eds) *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*. New York, Routledge.
- Lawson, S. (2013) Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics*. 10: 86–103. doi: 10.1080/19331681.2012.759059
- Libicki, M.C. (2009) *Cyberdeterrence and Cyberwar*. Arlington, RAND.
- Liff, A.P. (2012) Cyberwar: A new ‘absolute weapon’? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*. 35(3): 401–428.
- Limnll, J. (2014) Is Cyberwar real? Gauging the threats. *Foreign Affairs*.
- Lindsay, J.R. (2013) Stuxnet and the limits of cyber warfare. *Security Studies*. 22: 365–404. doi: 10.1080/09636412.2013.816122
- Lindsay, J.R. and Kello, L. (2014) Correspondence: A cyber disagreement. *International Security*. 39(2): 181–192.
- Lupovici, A. (2011) Cyber warfare and deterrence: Trends and challenges in research. *Military and Strategic Affairs*. 3(3): 49–62.
- Lynn III, W.J. (2010) Defending a new domain. *Foreign Affairs*. 35(3): 97–108.
- Maness, R.C. and Valeriano, B. (2015). *Coding Manual for v1.5 of the Dyadic Cyber Incident and Dispute Dataset, 2000–2015*.
- Maness, R.C. and Valeriano, B. (2016) Cyber spillover conflicts: Transitions from cyber conflict to conventional foreign policy disputes? In Friis, K. and Ringsmose, J. (eds) *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*. New York: Routledge.
- McEvoy Manjikian, M. (2010) From global village to virtual battlespace: The colonizing of the internet and the extension of realpolitik. *International Studies Quarterly*. 54: 381–401.
- Nye, J.S. (2010) *Cyber Power*. Cambridge, Belfer Center for Science and International Affairs.
- Oneal, J.R. and Russett, B. (1999) Assessing the liberal peace with alternative specifications: Trade still reduces conflict. *Journal of Peace Research*. 36: 423–442.
- Palmer, G., D’Orazio, V., Kenwick, M., and Lane, M. (2015) The MID4 Data Set, 2002–2010. *Conflict Management and Peace Science*. 32(2): 222–242.
- Pytlak, A. and Mitchell, G.E. (2016) Power, rivalry and cyber conflict: An empirical analysis. In Friis, K. and Ringsmose, J. (eds) *Conflict in Cyber Space: Theoretical, Strategic, and Legal Perspectives*. New York, Routledge, pp. 65–82.
- Rattray, G.J. (2001) *Strategic Warfare in Cyberspace*. Cambridge: MIT Press.
- Rattray, G.J. (2009) An environmental approach to understanding cyberpower. In Kramer, F.D., Starr, S.H. and Wentz, L.K. (eds) *Cyberpower and National Security*. Washington, DC, National Defense University Press, pp. 253–274.
- Rid, T. (2012) Cyberwar will not take place. *The Journal of Strategic Studies*. 35(1): 5–32.
- Rid, T. (2013a) Cyberwar and peace: Hacking can reduce real-world violence. *Foreign Affairs* (November/December).
- Rid, T. (2013b) *Cyberwar Will Not Take Place*. London, Hurst.
- Rid, T. and Buchanan, B. (2015) Attributing cyber attacks. *Journal of Strategic Studies*. 38(1–2): 4–37.
- Russett, B. and O’Neal, J. (2000) *Triangulating Peace: Democracy, Interdependence, and International Organizations*. The Norton Series in World Politics. W. W. Norton.
- Schneier, B. (2015) We still don’t know who hacked Sony. *The Atlantic*. Available from: www.theatlantic.com/international/archive/2015/01/we-still-dont-know-who-hacked-sony-north-korea/384198/ [accessed 5 January, 2019].
- Thompson, W.R. (2001) Identifying rivals and rivalries in world politics. *International Studies Quarterly*. 45(4): 557–586.

Correlates of state-sponsored cyber conflict

- Valeriano, B. and Maness, R.C. (2014) The dynamics of cyber conflict between rival antagonists, 2001–2011. *Journal of Peace Research*. 51(3): 347–360.
- Valeriano, B. and Maness, R.C. (2015) *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York, Oxford University Press.
- Valeriano, B., Maness, R.C., Choucri, N., Burton, J., Diehl, P.F., and Lindsay, J.R. (2016) Roundtable. *H-Diplo/ISSF Roundtable Reviews* XI(7).

3

CYBERED CONFLICT, HYBRID WAR, AND INFORMATIZATION WARS

*Chris C. Demchak**

Integrating thinking

Cybered conflict, cyber war, the Russian ‘hybrid war’ (Chivvis, 2001), and even the Chinese ‘wars under conditions of informatization’ (Polpeter, Chase & Heginbotham, 2017; Kania & Costello, 2018), all reflect the emerging reality of conflict among states in a deeply cybered, non-westernized world. Throughout history, the keys to conflict, competition, or war are the scale of available, relevant foreknowledge and of applicable resources to act accordingly. They are the critical ‘knowing and acting’ of all struggles, but in the emerging era, the volume of both foreknowledge and resources required is unprecedented. If one is constantly open to nasty surprises that can be imposed ubiquitously from one’s critical complex systems and one cannot gather the resources needed in time to mitigate, neutralize, recover from, and innovate beyond, the surprises imposed by adversaries, then one faces both exceptional uncertainty and wartime-levels of insecurity. Irrespective of what that struggle is called, one is then likely to lose in conflicts involving cyberspace. Just as in other eras and contexts, security in cyberspace is therefore not the absence of threats, but the inability to minimize either or both systemic uncertainty and the magnitude of significant harm associated with threats.

The current form of the global cyber substrate encourages long-running and obscured digitally-enabled contests that systemically blend uncertainty and insecurity. It offers five offense advantages for aggressive actors to employ in imposing their preferences on defending actors’ nation-wide socio-technical-economic systems (STES) (Demchak, 2012a). The multiplicative ways these five offense advantages – scale in organization, proximity, precision, deception in tools, and opaqueness in origins – can be employed in cyber campaigns has led to considerable confusion in terminology, observation, and weak theorization. Over the past decade, an explosion in debate the elements of the global internet and related technologies has produced an equally confusing number of new terms or labels. Practitioners and scholars alike have engaged in a good deal of ‘facet learning’, i.e. studying and reporting about one or two facets of a larger and much more complex whole without taking the final step of combining the facets. Missing is consensus about the basic

* All material is solely the author’s work and does not reflect any policy or position of the US Government, the US Navy, or US Naval War College.

nature of conflict through cyberspace. We lack an approach that helps explain conflict that is ‘cybered’ and its evolution.

This chapter aims to clarify the field by offering one basic term for the conflict now exploding in, through, and enabled by, cyberspace – ‘cybered conflict’. It is a form of large-scale intergroup or interstate struggle whose outcomes critically depend on the involvement of cybered means and whose activities lie upon a spectrum of traditional peace to war reaching all levels and actors in a state’s socio-technical-economic systems (STES). The goal here is to advance thinking systematically on the concept in order to promote better integration of a widely diverse array of arguments from differing disciplines, including economics which has eschewed directly addressing cybered conflict. This contribution is midlevel theory, offering the basic elements by which to move beyond mere observation to theoretically and practically framing productive, feasible implementations – to develop an integrative approach to both ‘knowing and acting’ in cyberspace for nations defending themselves in these struggles.

Four arguments will be made. First, cybered conflict’s central pursuit is the aggressive acquisition of access to accurate current data to ensure the overwhelming foreknowledge needed to control outcomes of a nation’s complex STESs. It is closely married to a virtuous loop in which more data means more resources, and more resources funds the acquisition of more data – as well as the available assets for action on the foreknowledge developed. That is, the cognitive – or ‘knowing’ – aspects of cyberspace ultimately will determine the uses – or ‘doing’ – to which its connectivity and content are put (Kuehl, 2007).

Second, the shoddy creation of the current cyberspace made this central pursuit much easier by expanding to a massive community of bad actors five offense advantages traditionally held largely by emperors and close neighbours. Put in other terms, emperors by the vastness of their resources could mass large armies, move great distances, apply a wide variety of weaponry over time, imperviously replace any lost resources, and remain at their home base immune to punishment or retaliation. Now any group of bad actors with access to the internet and time can execute cybered conflict campaigns using those advantages for minimal expense and with impunity.

Third, those states able to continually amass extensive foreknowledge of their own and of other states’ STESs – as well as the resources at scale to aggressively act in offense and defence – have underlying advantages in cybered conflicts. These are more likely to develop as cyber powers. The more robust the cyber powers are – i.e., the more state leaders manifest strategic coherence and appropriate scale in successfully developing national systemic resilience and legal forward disruption capabilities as needed, the more likely those states will prevail either as aggressors or defenders.

Fourth, the current world of cybered conflict is sorting into two futures. The most probably is a China-centric global system with minimally remaining, concrete democratic civil society influence. One aggressive, authoritarian actor – China – has already demonstrated the scale in resources (especially demographics) and strategic coherence in leadership to determinedly pursue systemic foreknowledge and to act institutionally on the data acquired globally. The fragmented and often fractious minority community of consolidated democratic states do not have individually either the scale of resources or strategic coherence necessary to prevail over time in cybered conflict given current trends that. Another possible future assumes that the rise of China cannot be contained in any case, but that there is a conceivable wary for the minority community of democratic states to persist in offering the world an alternative model. This future is only reasonably possible if these states make an existential choice to collectively erect a strategically coherent, cybered ‘peer’ institution to

defend and nurture a competing, completely transformed and economically vigorous cyberspace along democratic values and preferences.

This new world's struggles will move faster, hit further, change elements more profoundly, and amplify more broadly with more existential consequences precisely because of the new importance cyberspace awards to large scale acquisition of foreknowledge and resources married to STES strategic coherence. To date, democratic civil societies as a whole have been confused at best, complacent at worst, in dealing with this new world, their new role as a minority community, and the deep challenges to the assumed permanence of their global dominance and of democracy itself. This chapter offers an integrated way to view what has changed, what is happening, and the stark choices ahead for these societies and their thinkers in the coming deeply cybered world.

Aggressive acquisition of foreknowledge

Adversaries – whether state, proxy, or merely business competitors – have always sought information in advance to augment their own chances of prevailing in any form of contestation from war to gang or mafia deals to legitimate and rule-based markets (Handel, 1989). Having accurate data on what adversaries are planning to do, when, where, with what or whom, for how long and to what end is the gold standard of intelligence collection giving better chances of prevailing in pending, possible, or plausible struggles with others (Keegan, 2004).

The more complex and surprising the world surrounding competitors is, the more critical it is for adversaries to acquire and analyse vast amounts of data to provide accurate foreknowledge (Betts, 1982). In the cybered world, electronics are critical to the collection of this foreknowledge and, hence, to the cognitive analyses behind decisions in any form of competition or conflict (Arquilla, 2009). The further today's cyberspace spreads into all levels of any society, the more access points and systems a society's adversaries could penetrate and 'p0wn' (Oren, 2010) in the defending society's underlying cybered systems. It can be quite difficult to secure knowledge, especially it is transmitted to others; even verbal conversations can in principle be tracked by cameras and long-range listening devices (Riley et al., 2005). Even posted paper mail can be tracked digitally through a set of postal centre servers capable of reproducing a trail of probable communications between endpoints (Gill, 2006). Everywhere that information can be obtained remotely through digitally enabled means has become a possible target for adversaries' campaigns for foreknowledge.

Among state level adversaries especially, every aspect of the opposition's national social, technical, and economic sectors is in play, making cybered conflict a particularly broad-based system-versus-system struggle (Gilpin, 1981; Nye, 2017). Even the communications essential to commercial relationships and western markets – long considered during the Cold War and its aftermath to be off the table in national security discussions – have become part of campaigns to obtain foreknowledge for possible control of defenders' resources (Wilber, 2018).

One major state actor, China has a well-established reputation for aggressive and blatant foreknowledge acquisition campaigns (McConnell, Chertoff & Lynn, 2012). Its industrial industries' blatant tendencies to copy and market technologies by reverse engineering was so well known even in the 1990s that the agreement to let China join the World Trade Organization (WTO) in 2000 rested on Chinese promises to fairly open its markets to all investors and close off state subsidies. The Chinese market's enormous scale loomed so large that the fact that China nonetheless pursued technology and market foreknowledge aggressively was ignored by potential western investors for years. While continuing to violate its

WTO promises, China has advanced economically in considerable measure by requiring foreign firms to hand over their technical data – now including source code – in trade for access to Chinese consumers. It has refused to prosecute violations of international economic standards, including remote or insider theft of critical data from westernized industrial, technological, and other economic systems (Atkinson & Ezell, 2015).

Furthermore, this aggressive acquisition of data is embedded in the international business models of China's commercial 'state champions'. Those leaders fully understand the personalized and broader five-year strategic expectations that they will rise to dominance in their sectors in order to justify the national support they received (Li, 2016). To that end, vast amounts of resources are spent and enormous efforts to acquire foreknowledge have been aggressively pursued, particularly for the past fifteen years (Zhou, Lazonick & Sun, 2016). Repeatedly, Huawei – the Chinese telecommunications equipment state champion along with ZTE – has been accused of stealing massive amounts of intellectual property in the markets in which it has steadily risen, especially telecommunications backbone equipment (DOJ, 2019).

Westernized states, especially the United States, have also vigorously pursued foreknowledge of adversaries through digitized data acquisition, but not systemically on everything, especially corporations and citizens. Due to civil society restrictions, intelligence operations are generally narrower in scope. Forward searches tend to focus on foreign governments specifically (Nakashima, 2008). The central locus of computer knowledge in the US – the National Security Agency (NSA) – is restricted from any domestic collection of data. In the early 2000s and in order to catch terrorists inside the homeland, the US government proposed a more systemic domestic government data collection plan – Total Information Awareness (TIA). It was met with both ridicule, vigorous legal objections, and cancellation (Poindexter, Popp & Sharkey, 2003). Commercial westernized entities such as Google, Facebook, and Apple have more access to wide ranging STES information – albeit on their own customers – than the US government does. However, they openly appear to fight government requests to share large portions of it, generally citing privacy and reputation concerns. More recently the European Union has elevated individual privacy rights through its GDPR regulation – including the right to be forgotten online. The result is to make vast amounts of systemic STES data unobtainable by EU national governments in general (Albrecht, 2016). More recently developers of artificial intelligence – which requires enormous amounts of raw data on which its algorithms learn patterns and evolve decisions subsequently – have complained about the lack of available, real training data from all walks of life in westernized countries (Campbell, 2019).

As an adversary, therefore, China is likely to develop better foreknowledge of any given defending opponent. Not only is the Chinese vigorous program of AI development able to access massive amounts of data retrieved from abroad for training (Aitoro, 2019). China's leaderships have also inaugurated a social credit system tracking the acceptable behaviours of every Chinese citizen from social media to economic exchanges (Qin & Hernandez, 2018; Wright, 2018). New regulations now require all Chinese firms to be willing to respond to Chinese government intelligence requests as needed (Bandurski, 2017). Chinese AI advances will have cumulative big data advantages in the near future that westernized democratic developers will have to create by simulation in hopes of matching the AI training sets and learning. Correspondingly, China's political leaders have a greater likelihood of having a wider command of trends and decision concerns across leaders and STESs of other nations as its increasing mountain of data is processed more rapidly by its better trained AI algorithms.

Offense advantages from shoddy substrate

Globally critical to all the major sectors of nearly all societies, the underlying cyberspace substrate was built shoddily, written in quick-written, fault-tolerant code cheaper to produce and relatively easy to hack (Mills, 2010). The 1990s euphoric and naïve early days of the internet widely spread the idea that a brave new world of free, accurate information would ensue, making governments irrelevant, massively increasing prosperity for everyone, and assuring democracy as the dominant governance model everywhere the internet went (Rheingold, 1993; Norris & Jones, 1998; Benedict, 1991; Oyedemi, 2014).

The nascent commercial IT capital goods industry that built this insecure societal substrate did not see spreading democracy or security overall as their responsibility. Nor did the early internet seem particularly unsafe at the outset. Rather, information technology (IT) was promoted as historically special and unstoppable. The IT entrepreneurs argued their industry alone was – and should always be – free of government regulations because any restrictions at all would be harmful to innovation and the progress of the future world’s prosperity in general (Geer et al., 2003). The result was an explosive commercialization of the internet that was security-blind save minorly as a product functionality or a business intelligence issue. The web’s producers focused on commercial gains over competitors in speed of coding rather than quality. This argument – which continues today in the westernized states – adamantly opposed any government regulations requiring common standards for embedded security be met (Oxley & Yeung, 2001; Kinnersley, 2015).

The resulting substrate – poorly secured and oversold as it was – changed conflict by globally spreading five offense advantages that had previously been available only to wealthy emperors, superpowers, or close neighbours. With few resources save time and access to the internet, an aggressor can wield the superpower’s *scale of organization* through a botnet, live at any *proximity* from five hundred to five thousand kilometres from the victims and easily acquire previously high quality intelligence, and launch a variety of attacks at any level of *precision* in targets, time, duration, effects, or return benefits desired (Demchak & Dombrowski, 2011). Two more offense advantages developed as well: *deception in tools* and *opaqueness in origins*. Given the complexity of the global cyber substrate across cultures, governance, technologically diverse systems, and connecting protocols – plus the sheer volume of content per second, attackers have the opportunity to hide their tools to prevent interruptions or protections, and to obscure themselves to prevent punishment or retaliation.

These last two advantages are special bonuses for the average aggressor organization or even large states. Small or larger groups of bad actors may roam across the poorly secured global web and conduct attacks with impunity and a large potential for success. While historically a conventional attacker could not hide its weapons or generally its armies, in cyberspace both can be cloaked for a very long time.

With these advantages, attackers can be covertly hollowing or ‘poisoning’ the value chains sustaining the economics of a state for so long that whole nations could be losing a cybered conflict and not realize it. For example, automatic updates – a staple of today’s cybersecurity good practices – can themselves be corrupted, removing what is a basic line of defence against harmful losses from the web. For six months in 2018,

[s]omeone was able to modify a copy of the Asus Live Update Utility, hosted on the Taiwanese manufacturer’s backend systems, and sign it using the company’s security certificate, even keeping the file length the same as the legit version, to make everything seem above board. The update utility ships with every machine, and routinely upgrades

the motherboard firmware and related software with any available updates from Asus. When it checked in with Asus's servers for the latest updates, the utility would [automatically] fetch and install a backdoored version of the Asus Live Update Utility ... between June and November 2018, according to Kaspersky. That infected build of the utility was designed to spy on roughly 600 machines, identified by their network MAC addresses hardcoded into the software. ... [D]ubbed ShadowHammer ... a very sophisticated supply chain attack ... stayed undetected ... [in large part because] ... trojanized updaters were signed with legitimate certificates.

(Thomson, 2019)

The apparent ease of cybered conflict and the associated removal of data and thereby its economic value has elevated cyber insecurity to a tier 1 national security issue for major advanced economies (Cornish, Hughes & Livingstone, 2011). The losses from the economic sectors of the democratic civil societies alone are said to constitute the 'greatest transfer of wealth in human history' (Paganini, 2013). The French Senate has characterized these losses as the 'pillage' of the future of France economically (Bockel, 2012). In recent years others have estimated the losses to average 1–2% of the annual GDP of the advanced democracies (PWC, 2014). The estimates of losses have year on year been rising indicating a cumulative decline in the robustness of economic growth across the most targeted economies – the westernized civil societies (Verizon, 2017).

With these advantages intact as long as the current and shoddy structure continues, cyberspace changes conflict profoundly from the Cold War and its twenty-year aftermath. Cybered conflict now strongly influences the trends in the distribution of national economic, deterrent, and reputational power throughout the global system. From the 2010 Stuxnet (Gross, 2011), 2015 Black Energy (Liang et al., 2017) or the 2016 OPM data hack (Gootman, 2016), attacks sponsored by – and widely attributed to – other states are common without a victim nation's leaders demanding national mobilization to militarily strike back at hosting countries. Today there is a rise in the destructiveness of attacks with losses that – though large in implications – still remain below the threshold of the traditional war defined by the Law on Armed Conflict (LOAC) (Schmitt, 2013).

More and more attacks simply destroy data en masse. In both the 2014 Sony (Sharp, 2017) (attributed to North Korea) and the 2012 Saudi ARAMCO (Bronck & Tikk-Ringas, 2013) (attributed to Iran) attacks, data was deleted, and computers destroyed. Ransomware (Everett, 2016), for example, was initially viewed as a nuisance when it surged several years ago. More recently, through badly or intentionally poorly coded ransomware, the effective destruction of data is rising because it cannot be decrypted. This development reached global proportions in major attacks such as the WannaCryPetya and notPetya (attributed to Russia) attacks mid-2017 (Simmonds, 2017). The 2017 WannaCry global ransomware attack, for example, effectively destroyed everything it encrypted, since it had no decryption for payment mechanism (Ehrenfeld, 2017; Romine, 2017). With limited personal costs to these attacks – especially if sponsored by another state – new and existing actors are emboldened in general to seek more ways to exploit the substrate (Sanatinia & Noubir, 2015).

The destructiveness of cyberattacks continues accelerating as aggressors test the limits of national tolerances for unconventional attacks and losses without directly responding through highly public and direct punishment. These attacks blend cybercrime tools with the whole-of-society cybered conflict and appear designed to coerce particular states or large economic actors into complying with the desires of the originating state without the proof needed to escalate into a kinetic war (Maness & Valeriano, 2015; Demchak, 2013).

Harder cyber hits – perhaps across more sectors or deeper in domestic infrastructure – are more likely if previous efforts are not perceived to have the desired effects of sufficiently harming their targets. Assaulted firms do not fold or seem to be punished existentially by stockholders – Sony still exists, as do the major WannaCry victims Maersk and Saudi AR-AMCO. Large victimized firms continue today as if the cybered attack was of no consequence. In every other field of enquiry, such conditions—no repercussions for attacks and lack of evident harm in prior attack modalities—tend to increase adversary efforts to make the attacks more evidently painful. If merely losing money or risking client trust is insufficient, then the next – and already present – level involves destruction of something that systemically matters more than a single firm’s IP or financial resources. In addition to the now normal information disruption campaigns, Russia has been using cyberattacks on energy plants routinely for the past several years in the Russo-Ukrainian war with carefully timed and programmed outages. It now invades cell phone connections to identify grouped Ukrainian soldiers in the field for battlefield missile strikes (Haines, 2015; Limnell, 2015). Cybered conflict is therefore moving more readily towards the destructive end of the peace-war spectrum as aggressor nations become more skilled in it – more robust in their cyber power, especially in using the five offense advantages.

Robust cyber power

Being a ‘robust’ cyber power strongly advantages an actor in this endless struggle for foreknowledge and resources among adversaries, enabling one a better chance to prevail in cybered conflict campaigns under current conditions. Power – whether robust or weak – is widely misunderstood. Unlike the Cold War and aftermath definitions, national cyber power does not solely depend whether a state has a vigorous offensive cyber program with a reputation for successful individual operations. Merely having a cyber command does not make a state a robust cyber power. Rather, in a system-versus-system conflict that moves along a spectrum of peace to war, cyber ‘power’ varies as well along the spectrum of competence in defending the national STES, in addition to any ability to operate beyond borders into other nations.

This competence is composed of two major categories of efforts – the systemic resilience capability of the entire nation (Hathaway, 2013) and the forward disruption capabilities of the government. Both are critical and must be balanced in order for a state to accumulate cyber power. In any case, the larger, more complex, more sieved, more diverse, and more digitally integrated the nation involved, the greater the strategic coherence – and the sheer scale in available foreknowledge and resources – are required to be a robust cyber power.

Either authoritarian or democratic states can, in principle, achieve this robustness, but most states of the world are, at best, weak cyber powers, even those with some solid reputation for offensive cyber capabilities (Martins, 2018). Robustness in cyber is determined systemically by state leaders and actions that exhibit strategic coherence in recognizing – and acting successfully upon – the need to orchestrate, nurture, and innovate the cyber security of their nation’s entire STES. This challenge was hard in previous eras, and has proven to date nearly overwhelming, especially for the open internet societies. For example, the continuing loss in GDP growth already noted is an indicator of the weak level of cyber robustness of these victimized and largely democratic states.

Defending one’s STES is particularly challenging for any state, especially those already under assault. Due to the inherent shoddiness of cyberspace, the general sources of harmful systemic surprise for modern democracies doubled in the past twenty-five years – from two

to four. In the pre-cyber era, complex societal surprises came from individual enterprises (layer 1) or from collections of independent enterprises (layer 2) commonly seen in critical infrastructure industries. With the cybered era, however, now reaching into the nation's vital functions are a massive volume of independent, criminal 'bad actors' (layer 3) spread across the world, along with a much smaller more focused and organized group of exquisitely skilled 'wicked actors' or 'wizards' (layer 4) usually employed by states or international criminal organizations (Demchak, 2012b).

In particular, due to the five offense advantages of the current cyber substrate, it has proven extraordinarily difficult to curtail the inroads and successes of the bad actors and their wicked actor compatriots. The scale and coherence of effort needed has proven exceptionally difficult to rationalize at the strategic political level within national systems, and across the international community of nations (DeNardis & Raymond, 2013). The lingering early internet optimism has continued to stymie systemic and collective responses from democratic governments in particular. The westernized IT capital goods industry's argument that government interventions will destroy IT innovation and stall the economy has crippled nationwide defence responses. Ignored is obvious contrary evidence from China readily available from open media reports for nearly a decade. China continues year on year to rise economically despite it having a controlled internet and requiring government equity in all IT industry firms. So strong are these early images of the great new internet-led world order that private sector actors continue to refuse to coalesce with civil society government over the strategic need for both to take responsibilities in protecting their collectively existential national cyberspace and its value chains (Kohl, 2017).

Making matters worse, the underlying structure itself is exceptionally technologically and organizationally difficult to secure when the national STES is largely unprotected and fully open to the rest of the world's networks – across conflicting national legal systems, network controls and architectures, and cultural-cognitive presumptions. Any civil society seeking to defend its own national cyberspace faces a diversity of technological and proprietary challenges in orchestrating security at any level much greater than would otherwise have happened, had the original internet stayed largely within national borders and legal regimes (Powers & Jablonski, 2015). The overwhelming scale and variety of malignant cybered challenges – especially those by authoritarian states, their corporate state-champion proxies, and the huge state-encouraged criminal classes (in the case of Russia) – have overmatched the woefully out of date and inadequate defence tool chests of the formerly dominant civil societies.

For the first time in their collective history, the democratic allies do not have the proper mix in cyber power for defence and thus encourage the deepening of cybered conflict as adversaries experiment and learn what can be harmed at will. These adversaries can remotely remove or alter critical information and maintain backdoors for future actions from theft to destruction. Using the stolen IP or insider knowledge, they can bury, bribe, bully, or blackmail defending democratic corporate or political leaders. They can seem to legitimately displace the victim's industry assets in the market while having behaved badly out of sight of most observers.

The result is the hollowing of the nation's or group of nations' abilities over time to respond or advance technologically and economically over time, eventually politically as well. The best way to destroy a democracy is by destroying its economy; the tolerance, transparency, and inter-citizen/-institution trust vanishes rapidly, as demonstrated across Europe in the 1920s (Romer, 1992). While no state is a robust cyber power today, China has so far demonstrated the most strategic coherence in the use of its demographic and economic

scale to operate broadly and further its national security and economic interests. While the democratic states originating the internet struggle to even agree on cyber security, this rising authoritarian ‘anchor-state’ aggressively employs the five offense advantages through digitized proxies throughout the world. It succeeds in ubiquitously extracting massive amounts of STES data from other states, and is focused on acquiring the technology to rapidly process the data for foreknowledge and resource returns. It is well on its way to having a considerable head start in achieving robustness in cyber, and certainly its political leaders intend for it to be ‘the’ global cyber power (Inkster, 2018).

Future China-dominated international system *pur* or moderated? Existential challenge

Today the most likely future global world order is a leaning-authoritarian China-centric international system. Chinese scale and strategic coherence dominance across all key fields of technology (DeNardis, 2012) and economy stand poised to determine the shared daily practices and flows of economic resources globally. A second future is possible and will take considerable work on the part of practitioners, private sectors, scholars, and leaders across allied civil society democratic nations. This alternate future is a multi-grouped, largely mixed, vaguely larger China-permeated international system with at least one major regionally resilient democratic subsystem jointly operated by a prosperous minority of unified civil society states who defend and transform, their collective cyberspace into a securable, generative, and advanced democratic IT substrate and market open for trade but not exploitation or abuse. If the latter emerges with the means to rescue a remnant of what is vanishing today in terms of the global governance regime (Nye, 2012), then cybered conflict is likely to continue but with less existential consequences for the small number of consolidated democracies in the world. The advance of the authoritarian STES model and technology-infused governance preferences are more likely to be blunted for decades, buying time for the defences of the civil society states, the securable rebuild and adaptive resilience of their democratic IT, and the democracy aspirations of much of the developing world to be strengthened.

The trends behind China’s rise to central player in the more likely future international system are to a large extent inherent given China’s scale in its singular demographic weight and commensurate economic influence due to market size. But it is also a function of the strategic coherence of the Chinese leaders in the CCP whose instructions are largely accepted by the wider society. At the end of the day, barring global catastrophe, it is inevitable that such a state would rise to the centre of the global system of states (Yuan, 2018). China’s actions to control their own internet and society resonate favourably with the wider developing world in which democracy – if it has taken root at all – is a shallow import easily adapted to underling authoritarian leaning, affective cultures (Chaihark and Bell, 2004). For China’s governing structure, the five-year plans are adapted to an outside world in which Chinese firms operate. These are more ambitious, economically realistic, and technologically and economically advancing than such plans proved for the former Soviet Union (Chan, 2018). As the nation progresses, adherence to the ambitious objectives in these plans is expected by all economic and government actors, and rewarded across industries and provinces (though both are skilled in obfuscation of concrete or objective results) (Zhang, 2016).

When several five-year plans in a row place telecommunications industrial dominance as a key objective, the desired strategic coherence of the state is expressed unequivocally. The goals are mirrored in the industrial scale projects and ambitions among competing commercial and political leaders. Even state champions have to comply. They push the seams

in the existing international rules of economic exchange in order to rise globally through determination and persistent presence. They exploit state subsidies, legal immunity, gaps in regulations across nations, and questionable business practices already well known in China (including the 4 Bs of bribery, bullying, blackmailing, and hostile buying) (Demchak, 2017). For the more important of these firms, this effort has succeeded so far. The Chinese telecommunications giant, Huawei, was not among the top seven telecommunications corporations in the world in 2004. In 2019, it is now the first, second, or third depending on the specific sector (Fan & Gao, 2016) – an unprecedented rise and some would argue impossible without bad behaviours en route (Bastone, 2019).

In many respects, the China-centric globe without the countervailing prosperous democratic civil society model is already apparent inside the country itself. Resources flow to the centre – Beijing or designated regional capital, and the economic value chains are expected to be designed to ensure that happens. In such a world, all decisions that matter globally or specifically – according to the leaders in Beijing – will flow through some central node, perhaps a compliant UN, with China's right to *primus inter pares* if it chooses to sit at that discussion. China has a long history of 'vassalization' that, unlike the colonialization of Africa by the Victorian states, does not necessarily include regime change, but it does include an automatic veto and first bite at any apple if desired by Chinese representatives (Swanström, 2005; Cohen, 2006; Clarke, 2010). Given the ubiquity of the huge Chinese diaspora today, the coverage of those representatives will be extensive geographically. It will be strategically intense where Chinese national interests have been declared, including natural resources, especially energy and food, and advanced manufacturing (if it has not already been moved to China proper). Already Chinese leaders have shown a willingness to punish violators of their preferences across a myriad of issues relating to telecommunications, finance, space, and political speech deemed disrespectful by the Chinese regime.

Economic statecraft – especially coercive punishment for noncompliance – will be overt, pettier, and likely routinely more severe in the China-centric future. Many lower level decisionmakers representing the CCP will be given autonomy in, kudos for – and profit from – acting more vigorously in defence of Chinese interests (Blanchard & Ripsman, 2003; Blackwill & Harris, 2016; Norris, 2016). Overreach will happen but, since the critical political and senior economic leaders in the vassalized states' STESs will be in the Chinese-sphere of strong influence, resisting states will have difficulty mounting a credible unified political or economic response short of war. With no unfettered media, the grievances will be buried in government automated censorship or agencies, possibly also with the bodies of those who spoke to loudly or attempted to organize resistance. In short, major parts of the world are likely to present as quieter in global media terms, calmer in political struggles, more controlled in social behaviours, and more generally compliant with central preferences from Chinese representatives across sectors of interest in each state (McKune & Ahmed, 2018). What civil society would term routine 'bad' business and political practices such as nepotism, corruption, usurpation of rights, arbitrary search, confiscation, and seizure, cronyism, inflated or false reporting, deception, and brutal political control will mark the intra and interstate behaviours in the China-centric system lacking a democratic countervailing influence (Hannas, Mulvenon & Puglisi, 2013; Bradley, 2015; Haddad, 2016; Wong et al., 2017; Wang, 2017). There is a second possibility, however, of a moderating, even possibly mitigating global influence role played by a minority community of democracies. For this future to occur, this group must actively ensure that its members cannot be peeled apart and individually economically, technologically, or regionally vassalized by state-sponsored bullying, bribing, blackmailing, buying, charm offensives, or deception. The community must

trade with, operate in, and provide the international system with an alternative model of governance, security, and values. The consolidated democratic civil societies – despite being roughly 10% of the global population – could ensure their own wellbeing and survival by organizing collectively into a rough demographic peer to China and act with strategic coherence in key technological and economic areas. Especially critical would be institutionalizing the process of securing the cyberspace substrate by transforming it, and defending thereby the economic wellbeing dependent upon it.

Today western states' leaders are for the most part finally beginning to recognize the long-term national security implications of the true magnitude of those cyber-related economic losses. Only now has the United States formally included the defence of its economy as a national security mission for its key cyber unit. Only now has it, along with France most recently, recognized that defending its economic actors may require what was previously taken off the response table – persistently proactive cyber actions against foreign perpetrators. Individual national steps are, however, not enough to counter the scale of the assaults nor the urgency of the situation.

For the democratic civil societies, this deepening cybered conflict along with the rise of a more aggressive China now imposes an existential choice – hang together or most assuredly be separately, economically-technologically vassalized, and eventually marginalized globally. Needed is a more collective and comprehensively operational response for defending civil society powers to amass the countervailing systemic STESs foreknowledge and the scale of resources required to mitigate, neutralize, recover from, and innovate beyond the uncertainties and insecurities of the current shoddy cyberspace. Only by coalescing as a decidedly democratic force with 900 plus million people, operationally joined across key telecommunications and IT capital goods (as well as energy and finance) aspects of their interlaced socio-technical- economic systems can the minority community of consolidated democratic civil societies survive. This community must coalesce the requisite scale and strategic coherence necessary to have a reasonable chance of being recognizable prosperous and defensible democracies in 60–80 years.

Collective response essential in cybered conflict and needs research and action – CORA

Irrespective of how the future develops, and whatever cybered conflict is called, it will be a continuing source of uncertainty and insecurity for all states. For states that intend to survive as consolidated democracies, however, this conflict will be particularly hard unless the underlying substrate so poorly built is itself transformed into something defensible for democratic values and their value chains (Mallery correspondence, 2012–2019). These democracies have to alter the playing field of this kind of battle in order to make it less productive for adversaries. Whatever mechanism is created to ensure the survival of robust democracies in the coming system, the construction must begin soon to the narrative and the institutional structures in place and able to defend the intertwined STESs and their economic vitality.

First and foremost, the fractious advanced democracies will have to combine to build actionable scale and a collective strategic coherence. Given the rapidly growing losses in their economic wellbeing, these nations need to buy time for the R&D blitz needed to transform the shared cyberspace substrate underlying their allied environments into something defensible for democratic values and value chains, and still generative of economic and innovation advance. One particular mechanism – a 'cyber operational resilience alliance' (CORA) – offers both (Demchak, 2019). The alliance would link the telecommunications industries

with the IT capital goods industries with their respective governments and militaries in an operational, joined effort that defends all the allies and their cyber-dependent economic actors. In return for their commitment to the overarching goal of collective reduction in insecurity, the IT capital goods sectors are provided a 900+ million strong, single democratic community market free of authoritarian proxy corporate subversion, hostile or coerced ownership, or tainted business competition with no reliable legal protection. The CORA would make the joint, existing cyberspace substrate as secure as possible for now while coalescing the collective and massive investment across universities, industries, and governments needed for its transformation and the survival of civil society economies and values over the long time.

Considerable consensus, funded widespread research, and multi-sector accommodation and implementation are critical now. Whatever specific forms this conflict takes at any given moment, it will be a losing situation for those states who do not adapt and seek to change the terms of the conflict in their favour. The coming world advantages those actors able to obtain foreknowledge and resources at scale to develop robust cyber power and impose their preferences on others across the connectivity, content, and cognition elements of whatever technologies compose cyberspace in the future. China has already demonstrated what may be gained by having strategic coherence and scale; its role in this future world varies from central node to nearly central node in demographic, technological, and economic terms, barring global catastrophes. How that future resolves for democracy as a desired governance model and for democracies in the future as prosperous, defensible, and tolerant transparent societies greatly depends now on the research and actions by the scholars, practitioners, and leaders of those nations today.

Developing the collective action scale and strategic coherence of a CORA will take rethinking current assumptions about the international system, economic models, and the role of advancing technologies and complexity in national STES. This chapter takes both a deep and wide-angle view as a call for action by young scholars, experienced practitioners, and senior leaders in public and private sectors. It is time to integrate what we know not just from the past 10 years but also from systemic approaches in social, technical, and economic disciplines. Cyberspace – especially the heightened possibility of acquiring foreknowledge in unprecedented amounts, validity, and ease with impunity – has changed the conditions of human contestation, even if not the motives. Authoritarian states today use different terms than their counterparts in the democracies – such as hybrid war or informatization war, but they are widely experimenting and pushing aside the liberal internationalist assumptions of the post-Cold War era and the realist bipolar models from the Cold War period. It is time to discard much of the dated presumptions set in cement during those highly artificial circumstances of the US-USSR Cold War. New theories are needed in fields of economics, war, comparative social science, security studies, complex adaptive systems, politics, largescale technology systems, international relations, and the emerging field of STES studies in order to ensure the survival of democracy in the rising cybered and post-western global reality.

References

- Aitoro, J. (2019) NIST's Ron Ross on the state of cyber: 'We literally are hemorrhaging critical information'. *Fifth Domain online*. Available from: www.fifthdomain.com/dod/2019/03/29/nists-ron-ross-on-the-state-of-cyber-we-literally-are-hemorrhaging-critical-information/ [accessed 29 April, 2019].
- Albrecht, J.P. (2016) How the GDPR will change the world. *European Data Protection Law Review* 2.
- Arquilla, J. (2009) How to lose a cyberwar. *Foreign Policy online*. Available from: <https://foreignpolicy.com/2009/12/12/how-to-lose-a-cyberwar/> [accessed 10 June, 2019].

- Atkinson, R.D. & Ezell, S. (2015) *False Promises: The Yawning Gap between China's WTO Commitments and Practices*. Washington DC: Information Technology and Innovation Foundation, 2015.
- Bandurski, D. (2017) Xi Jinping's web of laws – three regulations introduced on May 2, 2017 are a sign that China's vision of centralised cyber control is coming together. *China Media Project*. Available from: <https://medium.com/china-media-project/chinas-web-of-laws-39cfa747019c> [accessed 10 June, 2019].
- Bastone, N. (2019) Chinese electronics giant Huawei allegedly offered bonuses to any Employee who stole trade secrets. *Business Insider online*. Available from: www.businessinsider.com/huawei-indictment-trade-secrets-2019-1?utm_source=reddit.com [accessed 10 June 2019].
- Benedikt, M. (1991) *Cyberspace: First Steps*. MIT Press.
- Betts, R. (1982) *Surprise Attack: Lessons for Defense Planning*. Washington, DC, Brookings Institution Press.
- Blackwill, R.D. & Harris, J.M. (2016) *War by Other Means*. Cambridge, Harvard University Press.
- Blanchard, J-M., F. & Ripsman, N.M. (2008) A political theory of economic statecraft. *Foreign Policy Analysis*. 4: 4.
- Bockel, M.J-M. (ed.) (2012) *Cyber-defence: A global issue, a national priority ('the Bockel Report')*. Defence and Armed Forces Committee on Foreign Affairs. Paris: Senate of the Assembly General of France.
- Bradley, J. (2015) *The China Mirage*. New York, Little, Brown and Company.
- Bronk, C. & Tikk-Ringas, E. (2013) The cyber attack on Saudi Aramco. *Survival*. 55:2.
- Campbell, C. (2019) 'AI farms' are at the forefront of China's global ambitions. *Time* (February).
- Chan, E. (2018) The 'made in China 2025' plan aims to break China's reliance on foreign technology and pull its hi-tech industries up to western levels. *South China Morning Post* (September 10).
- Chaihark, C. & Bell, D.A. (eds) (2004) *The Politics of Affective Relations: East Asia and Beyond*. Lanham, Lexington Books.
- Chivvis, C.S. (2017) *Understanding Russian Hybrid Warfare*. Santa Monica: Rand Corporation.
- Clarke, M (2010) China and the Shanghai Cooperation Organization: The Dynamics of 'new regionalism', 'vassalization', and geopolitics in Central Asia. *The New Central Asia: The Regional Impact of International Actors*. World Scientific Publishing Co. Available from: https://research-repository.griffith.edu.au/bitstream/handle/10072/42419/71382_1.pdf?sequence=1 [accessed 10 June 2019].
- Cohen, A. (2006) After the G-8 Summit: China and the Shanghai Cooperation Organization. *China and Eurasia Forum Quarterly*.
- Cornish, P., Hughes, R., & Livingstone, D. (2009) *Cyberspace and the National Security of the United Kingdom*. London, Chatham House.
- Demchak, C.C. (2012a) Cybered conflict, cyber power, and security resilience as strategy. In D. Reveron (ed.), *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, DC: Georgetown Press.
- Demchak, C.C. (2012b) Resilience, disruption, and a 'cyber Westphalia': Options for national security in a cybered conflict world. In N. Burns & J. Price (eds), *Securing Cyberspace: A New Domain for National Security*. Washington, DC: The Aspen Institute.
- Demchak, C.C. (2013) Economic and Political Coercion and a Rising Cyber Westphalia. In K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*. Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.
- Demchak, C.C. (2016) Uncivil and post-western cyber Westphalia: Changing interstate power relations of the cybered age. *The Cyber Defense Review*. 1(1).
- Demchak, C.C. (2017) Defending democracies in a cybered world. *Brown J. World Affairs*. 24.
- Demchak, C.C. (2019) We need a Nato/EU for cyber defense [Cora]. *Defense One online*. Available from: <https://medium.com/china-media-project/chinas-web-of-laws-39cfa747019c> [accessed 10 June 2019].
- Demchak, C.C. & Dombrowski, P.J. (2011) Rise of a cybered Westphalian Age. *Strategic Studies Quarterly* 5: 1.
- DeNardis, L. (2012) Hidden Levers of internet control: An infrastructure-based theory of internet governance. *Information, Communication & Society* 15: 5.
- DeNardis, L. & Raymond, M. (2013) Thinking Clearly about multistakeholder Internet governance. *Eighth Annual GigaNet Symposium*, Center for International Governance Innovation.
- Department of Justice (DOJ) (2019) Chinese telecommunications device manufacturer [Huawei] and its U.S. affiliate indicted for theft of trade secrets, wire fraud, and obstruction of justice. news release (January 28).

- Drezner, D.W. (2003) The hidden hand of economic coercion. *International Organization* 57 (Summer): 643–659.
- Ehrenfeld, J.M. (2017) Wannacry, Cybersecurity and health information technology: A time to act. *Journal of Medical Systems* 41: 7. Available from: <https://link.springer.com/article/10.1007/s10916-017-0752-1> [accessed 10 June 2019].
- Everett, C. (2016) Ransomware: To pay or not to pay? *Computer Fraud & Security*. 4: 8–12.
- Fan, P. & Gao, X. (2016) Catching up and developing innovation capabilities in China's telecommunications equipment industry. In Y. Zhou, W. Lazonick, & Y. Sun (eds), *China as an Innovation Nation*, Oxford, Oxford University Press.
- Geer, D. et al. (2003) Cyberinsecurity: The cost of monopoly. *CyberInsecurity Reports*. Available from: www.totse2.net/totse/en/technology/computer_technology/cyberinsecurit171812.html [accessed 10 June 2019].
- Gill, P. (2006) Not just joining the dots but crossing the borders and bridging the voids: constructing security networks after 11 September 2001. *Policing and Society*. 16: 1.
- Gilpin, R. (1981) *War and Change in International Relations*. Cambridge: Cambridge University Press.
- Gootman, S. (2016) Opm hack: The most dangerous threat to the federal government today. *Journal of Applied Security Research* 11: 4.
- Gross, M.J. (2011) Stuxnet Worm: A declaration of cyber-war. *Vanity Fair* (April).
- Haddad, J. (2016) Gordon H. Chang. Fateful ties: A history of America's preoccupation with China. *The American Historical Review* 121: 4.
- Haines, J.R. (2015) Russia's use of disinformation in the Ukraine conflict. *Foreign Policy Research Institute: E-Notes*. Available from: www.fpri.org/article/2015/02/russias-use-of-disinformation-in-the-ukraine-conflict/ [accessed 10 June 2019].
- Handel, M. (1989) *War, Strategy, and Intelligence*. Abingdon, Routledge.
- Hannas, W.C., Mulvenon, J. & Puglisi, A.B. (2013) *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation*. Abingdon, Routledge.
- Hathaway, M. (2013) *Cyber Readiness Index 1.0*. Great Falls, Hathaway Global Strategies LLC.
- Inkster, N. (2018) *China's Cyber Power*. Abingdon, Routledge.
- Kania, E.B. & Costello, J.K. (2018) The strategic support force and the future of Chinese information operations. *The Cyber Defense Review* 3: 1.
- Keegan, J. (2004) *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda*. London, Hutchinson 2004.
- Kinnersley, B. (2015) A Chronology of influential [computer] languages, the [computer] language list: Collected information on about 2500 computer languages, past and present, Available from: <http://people.ku.edu/~nkinners/LangList/Extras/langlist.htm> [accessed 10 June 2019].
- Kohl, U. (2017) *The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance*. Cambridge, Cambridge University Press.
- Kuehl, D. (2007) The Information revolution and the transformation of warfare. In K. de Leeuw (ed.), *The History of Information Security: A Comprehensive Handbook*. Amsterdam, Elsevier Science.
- Liang, G., Weller, S.R., Zhao, J., Luo, F., & Dong, Z.Y. (2017) The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems* 32: 4.
- Limnll, J. (2015) The exploitation of cyber domain as part of warfare: Russo-Ukrainian War. *International Journal of Cyber-Security and Digital Forensics* 4: 4.
- Mallery, J.C. & Demchak, C.C. Correspondence between 2012–2019.
- Maness, R. & Valeriano, B. (2015) *Russia's Coercive Diplomacy: Energy, Cyber, and Maritime Policy as New Sources of Power*. Springer.
- Martins, R.P. (2018) Punching above their digital weight: Why Iran is developing cyberwarfare capabilities far beyond expectations. *International Journal of Cyber Warfare and Terrorism*. 8: 2.
- McConnell, M., Chertoff, M., & Lynn, W. (2012) China's cyber thievery is national policy – and must be challenged. *The Wall Street Journal* (27 January).
- McKune, S. & Ahmed, S. (2018) Authoritarian practices in the digital age| the contestation and shaping of cyber norms through China's internet sovereignty agenda. *International Journal of Communication*. 12.
- Mills, E. (2010) In their words: Experts weigh in on Mac Vs. Pc security. *CNET online*. Available from: www.cnet.com/news/in-their-words-experts-weigh-in-on-mac-vs-pc-security/ [accessed 10 June 2019].
- Nakashima, E. (2008) Bush order expands network monitoring. *Washington Post* (January 26).

- Norris, P. & Jones, D. (1998) Virtual democracy. *Harvard International Journal of Press Politics*. 3.
- Norris, W. (2016) *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control*. Ithaca, Cornell University Press.
- Nye Jr., J.S. (2011) *The Future of Power*. New York, Public Affairs Press.
- Nye Jr., J.S. (2014) The Regime complex for managing global cyber activities, *Global Commission on Internet Governance Paper Series*. Available from: www.cigionline.org/publications/regime-complex-managing-global-cyber-activities [accessed 10 June 2019].
- Nye Jr., J.S. (2017) Deterrence and dissuasion in cyberspace. *International Security*. 41: 3.
- Oren, A. (2010) IDF dependence on technology spawns whole new battlefield. *Ha'Aretz*. Available from: www.haaretz.com/1.5081129 [accessed 9 June 2019]
- Oxley, J.E. & Yeung, B. (2001) E-Commerce readiness: Institutional environment and international competitiveness. *Journal of International Business Studies*.
- Oyedemi, T. (2014) Internet access as citizen's right? Citizenship in the digital age. *Citizenship Studies*.
- Paganini, P. (2013) Cyber-espionage: The Greatest transfer of wealth in history. *H+ Magazine online*. Available from: <http://hplusemagazine.com/2013/03/01/cyber-espionage-the-greatest-transfer-of-wealth-in-history/> [accessed 9 June 2019].
- Poindexter, J., Popp, R., & Sharkey, B. (2003) Total Information Awareness (TIA). *Aerospace Conference, 2003. Proceedings. IEEE* 6.
- Pollpeter, K.L., Chase, M., & Heginbotham, E. (2017) *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations*. Santa Monica: Rand Corporation.
- Powers, S.M. & Jablonski, M. (2015) *The Real Cyber War: The Political Economy of Internet Freedom*. Urbana, University of Illinois Press.
- Price Waterhouse Cooper (PWC) (2014) Global State of Information Security® Survey 2015. *Annual State of Information Security Survey*. Available from: www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml [accessed 10 June 2019].
- Qin, A. & Hernandez, J.C. (2018) How China's rulers control society: Opportunity, nationalism, fear. *New York Times* (November 25).
- Rheingold, H. (1993) *Virtual Communities: Homesteading on the Electronic Frontier*. Reading, Addison Wesley.
- Riley, K. et al. (2005) *State and Local Intelligence in the War on Terrorism*. Santa Monica, Rand Corporation.
- Riley, M. & Vance, A. (2011) Cyber weapons: The new arms race (the Pentagon, the IMF, Google, and Others Have Been Hacked. It's War out There, and a Cyber-Weapons Industry Is Exploding to Arm the Combatants). *BusinessWeek* (July).
- Romer, C.D. (1992) What ended the great depression? *The Journal of Economic History*. 52: 4.
- Romine, C.H. (2017) Bolstering government cybersecurity lessons learned from Wannacry. Testimony before US House of Representatives Committee on Science, Space, and Technology Subcommittee on Oversight and Subcommittee on Research and Technology. Available from: www.nist.gov/speech-testimony/bolstering-government-cybersecurity-lessons-learned-wannacry [accessed 10 June 2019].
- Sanatinia, A. & Noubir, G. (2015) Onionbots: Subverting privacy infrastructure for cyber attacks. 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks.
- Schmitt, M.N. (ed.) (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare* (TM 2.0). Cambridge, Cambridge University Press.
- Sharp, T. (2017) Theorizing cyber coercion: The 2014 North Korean operation against Sony. *Journal of Strategic Studies*. 40: 7.
- Simmonds, M. (2017) How businesses can navigate the growing tide of ransomware attacks. *Computer Fraud & Security*. 3: 9–12.
- Swanström, N. (2005) China and Central Asia: A new great game or traditional vassal relations? *Journal of Contemporary China*. 14: 45.
- Thomson, I. (2019) Spyware sneaks into 'million-ish' asus pcs via poisoned software updates says kaspersky – hackers were interested in 600 or so targets, it is claimed. *The Register Online*. Available from: www.theregister.co.uk/2019/03/25/asus_software_update_utility_backdoor/ [accessed 9 June 2019].
- Verizon (2017) Annual Data Breach Investigations Report. Available from: https://enterprise.verizon.com/resources/reports/2017_dbir.pdf [accessed 10 June, 2019].
- Wang, Z. (2017) The economic rise of China: Rule-taker, rule-maker, or rule-breaker? *Asian Survey*. 57: 4.

- Wilber, D.Q. (2018) China ‘has taken the gloves off’ in its thefts of U.S. technology secrets. *LA Times* (November 16).
- Wong, E., Chi, L.K., Tsui, S., & Tiejun, W. (2017) One belt, one road: China’s strategy for a New global financial order. *Monthly Review*. Available from: <https://monthlyreview.org/2017/01/01/one-belt-one-road/> [Accessed 9 June 2019].
- Wright, N.D. (ed.) (2018) *Ai, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives* [Whitepaper]. Washington, DC: US Department of Defense, JS/J39/SMA/NSI (December).
- Yuan, L. (2016) State, market, and business enterprise: Development of the Chinese integrated circuit foundries. In Y. Zhou, W. Lazonick & Y. Sun (eds), *China as an Innovation Nation*. Oxford, Oxford University Press.
- Yuan, L. (2018) Why made in China 2025 will succeed, despite Trump. *The New York Times* (July 4). Available from: www.nytimes.com/2018/07/04/technology/made-in-china-2025-dongguan.html [accessed 9 June 2019].
- Zhang, Y. (2016) Introduction: Dynamism and contention: Understanding Chinese Foreign Policy under Xi Jinping. *International Affairs*. 92: 4.

4

THE POLITICS OF STABILITY

Cement and change in cyber affairs*

Mika Kerttunen and Eneken Tikk

Introduction

Stability is a delicate attribute of public international order. If pursued to its absolute, it could paralyse the development and progress of humankind. If marginalized, it could fuel injustice, violence and conflict. Several differing concepts of ‘stability’ can be identified in international affairs. The United Nations Security Council uses the term to express a desirable state of affairs, almost synonymous with the concept of ‘peace’. In a 1992 ‘Note by the President of the Security Council’, various sources of instability were seen as threatening peace and security. The Council recognized that otherwise welcomed political changes may bring new risks to stability and security, especially stemming from changes to state structures. As the Council observed, ‘non-military sources of instability in the economic, social, humanitarian and ecological fields’ had become threats to peace and security (UNSC, 1992). Similarly, in 2005, the Council discussed the food crisis in Africa as a threat to peace, security and stability (UNSC, 2004–2007). In other contexts, the UN has identified ecological damage, disruption of family and community life as well as greater intrusion into the lives and rights of individuals as endangering stability (UNS-G, 1992). A 2017 Security Council Resolution affirmed that regional and bilateral economic cooperation and development initiatives play a vital role in achieving stability and prosperity (UNSC, 2017).

Inviting states to act in ways that can generate and support long-term, sustainable peace and set new thresholds for civilization, the Security Council believes that stability can expand the margins of peace. Here the Council aligns expectations of adherence to shared values and commitment to international obligations, not just regarding the actual absence of war and violence, but also in connection with sustainable societal and dignified human life. Individually, however, states may accept wider margins of insecurity between peace and conflict. Stability is an always-contingent condition towards which all states aspire,

* Adapted from Eneken Tikk & Mika Kerttunen (2019) *The Politics of Stability: Cement and Change in Cyber Affairs* (Oslo, NUPI 2019) by the kind permission of the Norwegian Institute of International Affairs. The original research was funded by the Norwegian Research Council research project GAIA of which the authors express their gratitude.

using highly individual formulas for determining what needs to be stabilized, why and how. Therefore, we hold that stability is a political arrangement.

Focusing on the interrelationship between international peace and stability, and ways of achieving both in the context of ICTs, we will offer a model of stability of cyberspace. We begin by examining the concepts of ‘stability’ and ‘strategic stability’ as understood with regard to international security. This conceptual analysis is followed a presentation of by the political claims of stability expressed in national and international cyber- and information-security discourses. Drawing on the conceptual approaches and the political claims, we then model the stability of cyberspace in three interlinked and reinforcing dimensions: 1) *equal and inclusive international relations*; 2) *prevention of war: the minimal peace*, with emphasis on averting a devastating nuclear war between the superpowers; and 3) the *functionality of global and national technical systems* and services. Defining stability in cyberspace only in the obvious terms of functionality – which we tend to detect – would be limited and politically utmost motivated. By that, we refer to sticking to a comfort zone where governmental responsibility to maintain global and regional stability will be side-lined. Indeed, we by our three-layered approach warn of the de-stabilizing nature of both operations and oppressive practices some governments are willing to take. Finally, we conclude with recommendations for action aimed at helping to create and maintain a stable – resilient and adaptive – cyberspace.

Stability in international security

In International Relations literature, ‘stability’ is not explicitly defined. The term frequently refers to a desired outcome of international order and a pre-condition of peaceful international and domestic life. When assessing or describing stability, scholars focus on three elements of the international system. First, they look at the *nature of the international system* – for example, as hegemonic, bipolar, or multipolar. Second, they enquire into the *means* or *institutions* designed for managing power relations within the international system – for example, the balance of power, hegemony, nuclear weapons (and deterrence), collective security, world government, peacekeeping, war, international institutions, international law, and diplomacy (Bull, 2002). Finally, they examine the *nature of international actors* and their interactions, typically seeing democracy and trade as stabilizing factors and the basis for the internal strength of states (Milner, 1998, p. 112–123; Hasani, 2002).

According to Deutsch and Singer (1964), systemic stability increases the likelihood of the (international) system retaining its essential characteristics. In a stable international system, no single nation can become dominant, while the survival of the most members (states) is ensured and there is no large-scale war. Consequently, stability, for a single state, represents the probability of its ‘continued political independence and territorial integrity without any significant probability of becoming engaged in a war for survival’ (Deutsch & Singer, 1964, pp. 390–391). Hurwitz’s (1973) five propositions – absence of violence, governmental longevity/endurance, existence of legitimate constitutional order, absence of structural change, and multifaceted societal attributes – help to operationalize stability. Dowding and Kimber (1983), criticizing views that regard stability as *regularity* of behaviour and *normalcy* in affairs, emphasize the capacity of a political actor to prevent incidents and threatening contingencies ‘from forcing its non-survival’. Drawing on biology and physics in studying security and survival, Boyd (1976) stresses that closed systems inevitably develop entropy that in turn will cause a systemic change, the destruction of the old and the creation of something new. Similarly, Gaddis (2018) regards controlled environments as unable to cope with the breakdown

of controls – ‘as they sooner or later must’; further, he holds, the assumption of stability blinds us to acknowledging, accommodating and recovering from change or disturbance.

Fundamentally, therefore, stability concerns an entity’s capacity to resist unavoidable threats and accommodate to inevitable changes. The latter can vary between required and unanticipated transformations. This conceptual understanding acknowledges the continuity of systemic functionality as the most important objective. In this view, stability does not equate to any particular *status quo*, even if one is set as the aim or example for a discourse – especially in political speech focusing on a cemented political or world order. Although stability may align with *status quo* in some circumstances, given the inherent systemic dynamics and specific cyber-technological developments, it is important to acknowledge the likelihood and imperative of constant change. Moreover, stability in its purest form, successfully denying change, necessarily remains a temporary phenomenon, even an ahistorical illusion.

Consequently, no single trend, event, or measure is necessarily stabilizing or destabilizing. In economics, abrupt or wide fluctuations in the values of currencies or commodities may slow export or import, supply or demand, thus destabilizing the functionality of the market as well as national and individual economies (e.g. *The Nation*, 2016)). While escalation of a confrontation might, in general, be considered destabilizing, in the nuclear deterrence literature the risk of escalation is considered to promote stability (Ogilvy-White, 2011). Moreover, some scholars regard the proliferation of nuclear weapons as stabilizing, others are highly destabilizing (Sagan & Waltz, 2003). The development of national and military cyber capabilities may seem alarming. However, these developments can also be seen as strengthening national systemic resilience, the ability to accommodate technical and behavioural changes, and as supporting responsible, predictable state behaviour.

Stability in international relations

Stability is much sought after in international affairs. Our analysis begins with the US–USSR/Russian superpower relationship, where the idea of ‘strategic stability’ was first acknowledged. From that dense nuclear relationship, we move to recent claims concerning stability that governments have presented regarding the ICT environment. Before examining specific means of achieving stability, we look at the technical concerns of stability/instability, a highly relevant aspect in the ICT environment shared by all countries.

Strategic stability

A particular reading of stability, the concept of *strategic stability*, emerged as the United States and the Soviet Union became engaged in a nuclear arms race in the 1950s. Fears of a devastating surprise attack drew attention to vulnerabilities, and to mutual capabilities to retaliate (Wohlstetter, 1958 and 1959; Schelling, 2013; Gerson, 2013). In a very twisted way, the existence of a certain degree of instability, especially accepting the risk of escalation, became seen as ensuring security – or the avoidance of major war – in the nuclear era (Ogilvy-White, 2011).

Strategic stability functions as a pattern of thought fundamental to the theory and policy of deterrence. It has become a cornerstone of superpower relations. For Arbatov (Arbatov et al., 2010) strategic stability indeed refers to the stability of strategic nuclear equilibrium maintained for a long period of time and despite the influence of destabilizing factors. The concept is dualistic, dynamic and contextual. It operates with the desire for survival and the knowledge of vulnerability as well as change and continuity. It directs actors to take into account their own capacities but also those of their adversary. It recognizes the need to look at

technical details and objective facts but acknowledges that these will change. Strategic stability has traditionally centred on nuclear weapons, but can also have application beyond them.

The demise of the Soviet Union and the dissolution of the Warsaw Pact did not change the understanding of strategic stability in international politics. The political, economic and military rise of the People's Republic of China has only solidified the system centred on nuclear and strategic weapons. USA–Russia and USA–China relationships and an stance of arms control continue to function as the main conditioning framework for questions of both the established nuclear situation and emerging security/stability questions. For example, the US Nuclear Posture Review (NPR) lists the maintenance of strategic deterrence and stability at reduced nuclear force levels as one of its goals. It goes on to note that bilateral dialogues with Russia and China on missile defence, space-related issues, conventional precision-strike capabilities, and nuclear weapons issues promote more stable and transparent strategic relationships (Rose, 2014).

We argue that the Russo–US strategic relationship has continued to be determined by the mutually acknowledged ultimate value of strategic stability. Here, as for the rest of the humankind, the question is one of survival. Perversely, our continued societal and biological existence is apparently held to be a function of the survivability of the US and Russian strategic weapons and command and control systems (Kazi, 2017; Krisnamurthi, 2017).

Stability for the ICT environment

In 1998, Russia explicitly notified the United Nations of the potential use of information technologies and weapons ‘for purposes incompatible with the objectives of ensuring international security and stability’ (UNGA, 1998). The Kremlin wanted to call attention to ‘actions taken by one country to damage the information resources and systems of another country while at the same time protecting its own infrastructure’—a thinly veiled reference to US information warfare policy and doctrines, and its dominant technological and military position. Further, Moscow warned of ‘the destructive “effect” of information weapons, which may be comparable to that of weapons of mass destruction’. To mitigate this perceived threat, Russia put forward a draft UN General Assembly Resolution that invited discussion on this and the development of ‘international legal regimes to prohibit the development, production or use of particularly dangerous forms of information weapons.’ (UNGA, 1998)

In line with this emphasis on bilateral superpower relations, the information security doctrines of the Russian Federation (2001, 2008 and 2016) have called for the maintenance of strategic stability, increasingly seen as threatened by the development and use of information and communication technologies. Here information security is set as a strategic objective to serve strategic stability and ‘equal strategic partnership’, with the purpose of creating ‘a sustainable system of conflict-free inter-state relations in the information space’ (RU, 2001, 2008 and 2016). Furthermore, Russian information security doctrines have explicitly emphasized the importance of domestic political, economic and social stability, as well as the stability of state authority (RU, 2001, 2008 and 2016).

In the UN, Russia has consistently underlined sovereignty and non-intervention and non-interference in the internal affairs of other states. The ‘Arab Spring’ and the ‘colour revolutions’ in the former Soviet republics of Georgia and Ukraine have kept the Kremlin cautious on the virtues of digitalization (Romashkina & Zagorskii, 2016). Advanced information and communication technologies – the Internet in particular – have been regarded dangerous, albeit useful, tools of subversion, information operations and the destabilization of internal order. The *international code of conduct* launched by Russia and China together with

four Central Asian partners notes that the development and application of new information and communication technologies have the potential for being ‘used for purposes that are inconsistent with the objectives of maintaining international stability and security.’ The six signatories call on nations to pledge that information and communications technologies and information and communications networks will not be used to interfere in the internal affairs of other states or with the aim of undermining their political, economic and social stability (UNGA, 2015). Moreover, so as to particularly emphasize domestic stability, the Russian-sponsored resolution (A/73/27) that mandated the UN Open-Ended Working Group in 2018 (UNGA, 2018) recalled a 1981 UNGA resolution, ‘Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States’, with language that Western liberal democracies find distasteful (UNGA, 1981).

The imperatives of national security and domestic stability and the ambition to remain a powerful strategic actor, on a par with the USA and beyond, have surfaced in Russia’s calls for digital sovereignty and emphasis on national media sphere, national segments of critical infrastructure, and a separate, national Internet, *RuNet*. The Russian *Doctrine of Information Security* included in the key objectives ensuring ‘information security in the field of strategic stability and equal strategic partnership’ and the protection of the sovereignty of the Russian Federation in information space through nationally owned and independent policy, and the development of a national system of Russian Internet segment management (RU, 2016). A separate national information system would allow maximal control over the Internet routing architecture in Russia – and the flow of information in the networks (Ristolainen, 2017). The aim has also been to secure Russian networks, and the confidentiality, integrity and availability of information within, from external influences and attacks (RT, 2019).

In its network policy, Moscow has been following Beijing. The ‘Great Firewall of China’ filters and censors Internet traffic by blocking access to certain IP addresses, hijacking certain DNS addresses to lead the inquiry to false sites, and keyword filtering aimed at preventing connection to the desired website. As stated in China’s 2016 *National Cyberspace Security Strategy*, Beijing sees networks as being used to ‘interfere in the internal political affairs of other countries, to attack other countries’ political systems, incite social unrest, subvert other countries’ regimes, as well as large-scale cyber surveillance, cyber espionage and other such activities.’ Moreover, political stability is regarded as a ‘precondition for national development and the happiness of the people’ (CN MFA, 2017; Zhuang Rongwen, 2018). Kazakhstan follows its partners. Its *Concept of Information Security* divides national information security into technical and socio-political aspects. The technical aspect involves ensuring the protection of information resources, systems and infrastructure; and the socio-political aspect focuses on the protection of national information space and systems of mass information (KZ, 2011; Azamatova & Balpanova, 2017).

As for the USA, the White House 2011 *International Strategy for Cyberspace* regarded stability as the continuation of expected and accepted norm-guided behaviour. It implicitly refers to the nuclear realm by noting: ‘in other spheres of international relations, shared understandings about acceptable behavior have enhanced stability and provided a basis for international action when corrective measures are required’. The US *International Strategy* pays great attention to the functionality of the global network, ‘rooted in the technical realities of the Internet’, and as a common interest (US, 2011, pp. 9, 22).

Echoing the understanding of the danger of unpredictability and surprise in international relations that guided Schelling’s thinking on strategic stability (Schelling, 1958 and 1960), the 2013 ‘U.S.–Russia Cooperation on Information and Communications Technology Security’

spoke of the need to ‘reduce the possibility that a misunderstood cyber incident could create instability or a crisis in our bilateral relationship’ (US, 2013).

The 2014 report of the US Department of State’s International Security Advisory Board on cyber stability recognized the importance of enhancing the ‘continuity of relations between nations in the face of attack or exploitation through cyber means’. The Board defined stable cyberspace in the best neo-liberal terms as:

An environment where all participants, including nation-states, non-governmental organizations, commercial enterprises, and individuals, can positively and dependably enjoy the benefits of cyberspace; where there are benefits to cooperation and to avoidance of conflict, and where there are disincentives for these actors to engage in malicious cyber activity.

(US, 2014)

This report emphasizes cyber stability as fundamentally depending on transparency and the knowledge on both sides (USA and Russia) of their opponent’s trigger points – actions that would lead to escalatory decisions and the deployment of more powerful capabilities, which in turn may result in full-spectrum conflict. Fostering transparency, attribution, and the political will to act are regarded as the critical underpinnings of cyber stability as well as the geopolitical, economic, technological, and legal elements of the cyber-stability framework. To avoid unintended escalation, the Board advocates setting rigorous rules of engagement for US military and civilian organizations in responding to significant attacks using cyber means.

Following the logic of the late 1980s, US–Soviet armed forces talks and the 1989 Agreement on the Prevention of Dangerous Military Activities, Russia has been proposing military-to-military dialogue and negotiations to prevent accidental cyber conflict between the two states. Washington has not responded to this call (Streltsov & Smirnov, 2017). Moreover, Streltsov and Smirnov claim that numerous other initiatives Russia has put forward ‘within the framework of the U.N. aimed at a joint work to examine global aspects of strategic stability, including in cyberspace’ have not been ‘taken into account’.

We argue that the US reluctance to enter sign up to such a regime, or indeed to any other cyber treaty, stems from Washington’s still-perceived position of superiority, which is not to be curbed. Both the Putin and Trump administrations are clearly not satisfied with the current state of arms-control measures: President Trump more in the nuclear domain, and President Putin more in the cyber domain.

Expressing their views at the UN First Committee (Disarmament and International Security) in 2017, various countries approach stability in terms of contingent, perceived problems. Factors seen as destabilizing include the arms race, inequality, unilateralism, and the build-up and deployment of military capabilities. Their statements outline a typology of stability consisting, as expressed by the national representatives, of general, comprehensive, strategic, economic and infrastructure stability. However, there is variation in the measures preferred for reaching, maintaining or strengthening such stability.

Western states promote international stability framework in and for cyberspace. This is seen as based on the application of existing international law, agreed voluntary norms of responsible state behaviour and confidence-building measures, supported by coordinated capacity-building programmes (Bird, 2017; Cleobury, 2017; Körömi, 2017). In its 2018 *National Cyber Strategy*, the USA sees stability as a function of international law and voluntary non-binding norms of responsible state behaviour in cyberspace. However, it places heavy

emphasis on strength: the capacity to deter, respond to and entail consequences against those who do not adhere to the framework (US, 2018; Kerttunen, 2018).

Libicki (2012) regards cyber capabilities as incapable of endangering strategic stability. His main argument is that, as the employment of cyber capabilities cannot create devastating effects, the survival of the victim state is not endangered, and the availability of its cyber capabilities and conventional or nuclear weapons can be jeopardized for only a short time. Such a situation, involving limited damage and temporary harmful effects, does not necessarily demand quick response or retaliation. However, he acknowledges that the concept and perception of cyberwar have 'created new ways to stumble into war'. This risk stems from the uneasy equation between the misperceptions of the one side, and the hypervigilance of the other: states react partially blindfolded and out of fear. Moreover, an attacker may calculate that, by a decisive and surprising cyber- or cyber-supported attack, it can gain an advantage which the victim state will be afraid of escalating further. Furthermore, Libicki mentions that if a cyberattack does not achieve its objective, the victim state may not have an incentive to retaliate, and that is contingently stabilizing. We feel, however, that such shadow-boxing represents dangerous cyber-brinkmanship where fear, misperceptions, and false assumptions not only endanger stability but also threaten peace.

Stability in cyber-physical environment

Common to superpowers, liberal democracies, and authoritarian regimes alike is the emphasis on securing essential technical national, industrial and information and communications systems in the name of stability. Again, the precise objectives and preferred mechanisms will vary. Protecting of critical information infrastructure is a common area of emphasis in national cyber and information security strategies (Kerttunen, 2019; Kerttunen & Tikk, 2019). Armed forces want to protect their information, communication, command, intelligence, navigation and early warning systems. Countries with nuclear weapons are particularly concerned about the survivability and credibility of their warning, weapons and command and control systems. Technical stability is thus a factor in both political and strategic stability. Given the technological nature of the ICT environment, and the inherent vulnerability of network, systems and services to intentional and accidental disturbance, ensuring technical stability is an essential aspect of stability in cyberspace.

ICTs have become the subject of international security dialogue as societal, economic, political and, increasingly, military functions have come to rely and depend on them. In most societies, dependence on ICTs is far greater than actual preparedness to safeguard their functions. Unsurprisingly, then, reports of cyberattacks and the development of military cyber capabilities readily give rise to angst in nations and populations.

Should ICT infrastructure be affected by a deliberate or accidental incident, there is a logical order in which services and functions fail or are recovered. Where resources to sustain online services are limited, priority will be given to critical infrastructure, services and functions. Accordingly, states have been called on to identify their critical infrastructure and services and assign responsibilities for maintaining the functioning of such infrastructure in time of crisis or emergency. Critical infrastructure and services concern assets, systems or parts thereof which are essential for the maintenance of vital societal functions, like the health, safety, security, economic, and social well-being of the population; the disruption or destruction of these would be expected to have a significant impact (EC, 2008).

For stability, two further considerations are essential. First, the more societal routines rely on ICTs, the more would a failure disrupt the rhythms of life. Such scenarios are generally

omitted from considerations of serious international consequences or remedies, as they would concern what might be seen as a ‘non-essential’ function. However, if several such functions were simultaneously and/or protractedly disrupted, affecting a significant population, that would in fact constitute a serious stability challenge.

Second, the ‘luxury’ factor of ICTs should not be underestimated. The non-availability of services and applications with little or no direct value to the state affected by a cyber incident may evoke significant reactions among the populace, spurring expectations towards the authorities who may be focused on dealing with the more serious consequences of the same situation. Such ‘no-access-to-Facebook’ situations should be included in contingency planning, as should potential fake and deep-fake campaigns exploiting the situation.

Applying a liberal reading to ICTs in global and domestic relations, the Obama administration’s 2011 *International Strategy for Cyberspace* operationalized network stability as a condition or state in which states:

- respect the free flow of information in national network configurations,
- ensure that they do not arbitrarily interfere with internationally interconnected infrastructure
- continue to recognize the domain name system as a key technology that needs to remain secure and stable.

(US, 2011)

The Trump administration has promised to offer to other governments advice ‘on infrastructure deployments, innovation, risk management, policy, and standards’, to further the global reach of the Internet and to ensure interoperability, security and stability (US, 2018, pp. 25–26).

Perhaps the clearest action aimed at securing the integrity, functionality and stability of the Internet is the Dutch initiative to protect the public core of the Internet (Broeders, 2015). The initiative calls for states to exercise restraint and reserve ‘in matters of national security versus the interests of the collective Internet’ as ‘the only way to guarantee the stability of the net in the long term’. The Dutch, however, also note that in reality, ‘those entrusted with national security are more likely to want to extend their reach than show restraint’.

The ICT environment is man-made. Thus, it is possible, to some extent at least, to insulate and isolate a country and its people from the Internet and foreign influence. In the search for stability, such ‘black boxes’ have been employed and are being designed. An anecdotal disagreement is attributed to Singapore’s former Prime Minister and strongman, Mr Lee Kuan Yew. For him, the American black boxes meant the ability to constantly reinvent themselves (as related in Sullivan, 2019).

In conclusion: recommendations for optimizing stability

Stability is never absolute, or set in stone. Each phase carries the elements of its own change, perhaps even its destruction. Furthermore, stability measures – like any political choices – involve deliberate risk-taking and imperfect measures, limited by their scope and effect.

There is no universal stability – or formula for such a thing. The values and objectives of the real-world politics of stability are contingent. Even the most directly technical recommendations for increasing systemic stability encounter the political imperatives of influence, power and resource allocation. The various measures examined above show clearly there is no single path to international peace, security and stability. Indeed, any individual measure

on its own might become a destabilizing factor. The objectives and measures of stability become accepted as real and true only by means of negotiations. In such negotiations, countries' positions on stability are conditioned by their national ambitions and preferences as to the means and ways to achieve those ambitions, and stability, as necessary.

Those who genuinely seek stability must not leave its framing to chance. Guidance for behaviour aimed at producing greater stability should, at the very least, explain what the proposed norms are intended to achieve, and how; and how these outcomes relate to international and national stability. Account must also be taken of the feasibility of implementing the proposed norms without adversely impacting the balance of markets and technical solutions. Without such assessment, and relying on best-guess approaches, it is impossible to guarantee a move towards stability. In a worst-case scenario, further instability may be created.

Combining the domestic, strategic and technical imperatives of stability, a minimum task of international stability measures can be defined as follows: to create conditions in which serious political-military conflict can be averted, international political relations are continued, and the functionality of global techno-strategic systems, networks and processes is maintained. This minimalist reading of stability of cyberspace focuses on the avoidance of major catastrophes and a devastating war 'in our time'. A maximalist reading would call for tools to accommodate and embrace change: more sustainable stability, encompassing the concerns of human life and societal empowerment. In any case, all the three legs of stability, *peace*, *equality* and *functionality* need to be firm. Despite their mutually amplifying relationship, the three dimensions are analytically distinct, as they assume different agent-structure relationships, entail different empirical challenges and imply different solutions.

Today's emphasis on voluntary non-binding norms, rules and principles is amenable to both the USA and Russia, otherwise acknowledged as fierce rivals in the international cyber dialogue. Washington has no desire for any kind of 'cyber treaty', and Moscow wants to avoid authoritative references to state responsibility, international humanitarian law and self-defence in the ICT environment. Avoiding, not answering, open questions of the applicability of international law in cyberspace, the USA and Russia effectively control the global operating environment. Other governments are flooded with the views of global commissions and conferences, contrasting scholarly pronouncements, competing governance models, and technological assistance packages, all aimed at ensuring the desired kind of 'modernity'.

In this game of influence, stability is as much being shaken as it is claimed to be sought after. The emphasis on sub-optimal solutions supports the reckless cyberspace operations of the most powerful and the most eager governments. This opportunism is in fact a manifestation of cyber-brinkmanship where the assumed void of rules and responsibilities is exploited, and the tolerance of others is tested. The hope is to forge a new equilibrium without being caught – and without major catastrophes.

The vast majority of governments do not subscribe to this military-dominated reading of cyberspace, international law and confidence building (Kerttunen & Tikk, 2019). Most governments have no intention of becoming engaged in aggressive cyberspace operations: indeed, they have their hands full, trying to deal with sustainable development, economic prosperity and human and societal empowerment. They do not need the sub-optimal peace, security and stability measures that wish major catastrophes away. What do they need – optimal peace, security and stability to resist and recover from human-caused technical incidents, the negative effects of cybercrime and the harmful effects of a few indifferent governments. Never among the fittest, these governments need the most advanced form of

stability in order to survive: the ability to accommodate change. Today's global politics of stability cannot guarantee this.

States must to take stability in cyberspace seriously. Emphasizing the continuity of operations and stability as accommodating change, we propose the following package of normative and capacity-enhancing measures. No single measure can solve the problem.

On the normative side, the military-heavy narrative and politics of cyber affairs must be replaced with an agenda for peace and development. Simultaneously, there must be greater efforts to strengthen the international and domestic rule of law, including the development of international law in behaviour in and through cyberspace. The aim of this dual move is to return to the promise of ICT as tools of peace and prosperity, a promise that had been lost amidst the events in Estonia 2007, Georgia 2008, Stuxnet, Snowden, Cambridge Analytica, and the ruthless practice of cyber espionage. This move is what UN Secretary-General António Guterres outlined with his September 2018 *Strategy on New Technologies*: a deepening understanding of how new technologies can be used 'to accelerate the achievement of the 2030 Sustainable Development Agenda and to facilitate their alignment with the values enshrined in the UN Charter, the Universal Declaration of Human Rights and the norms and standards of International Laws' (UNS-G, 2018).

The Internet must be kept free, open, safe, and united (see Clarke & Knake, 2019). We need to support the continuation of expert and multi-stakeholder-centric Internet governance model, with its established track record of maintaining and developing the Internet. Any deviation from this model is likely to exacerbate the digital divide – reducing the economic and societal promise of the Internet and leading to insecurity and instability. True, China and Russia have chosen a path that effectively controls and limits flow of information across and within their on-line and off-line borders. Their approach is lucrative for those who believe that digitalization is dangerous and that cemented solutions offer best stability. We recognize that competing cybersecurity governance models are emerging, but question the sustainability and stability of closed systems.

For dealing with recurrent crises and conflicts, institutionalized mechanisms must be established that regionally and globally address issues of political and technical instability. The former includes the continuation of global and/or bilateral cyber consultations; the latter not only transparency and cooperation but also the greater application of stability-enhancing restraint measures. Importantly, preventive diplomacy – not responses or countermeasures – must be acknowledged and developed as the primary toolbox for international relations in today's world.

To enhance national cyber capacity, we recommend *resilience first, and resilience for all*. The world's developing countries lack the financial, human and technical means to maintain and upgrade their technologies. To avoid deterioration of local and global connectivity, thereby losing its political and economic benefits, the West needs to launch robust and sustained transfers of advanced technology aimed at bridging the digital divide and the concomitant injustice and insecurity. Technologies are needed – to safeguard and sustain networks and services, but also to establish robust and resilient platforms across society, making it possible to achieve vital developmental goals. Technology alone is insufficient: investment in the development of individual and organizational skills, competences and performance is needed – without the newly trained workforce migrating to the West. This bold move will also help to undermine the Russian and Chinese promotion of stricter governmental controls.

No single measure or feature is in itself stabilizing or destabilizing. However, greater transparency about the root causes and modalities of ICT vulnerabilities, as well as cyber operations, can be expected to have broader stabilizing effects, triggering more focused efforts,

at the national and international levels, to detect and eliminate acute sources of threat and insecurity.

To support this technological surge, domestic, regional and global dialogue and enhanced cooperation on matters of ICT development and employment must be maintained. Basically, we need to ensure the continuity of technical and political operations to handle threats and incorporate technical and societal development. This work calls for international capacity-building that applies known standards and criteria, but is sensitive to contingent needs. Finally, capacity and stability rest on human cognition. Academic and professional programmes for the maintenance and development of systems and services must inculcate norms of normalcy and decency, and emphasize non-escalatory solutions to destabilizing incidents.

As long as there is no shared understanding of what the problem is or the issues that the proposed measures are to prevent, solve or mitigate, any answers must remain conditional and limited. Conceptually, and seen from a systemic perspective, stability has intrinsic, absolute value in its own right. In practice, and seen from actor perspectives, stability becomes instrumental, contingent – and always imperfect. Any stability argument or measure will always be based on the fundamental values and belief system of the speaker in question.

References

- Arbatov, A.G., Dvorkin, V.Z., Pikaev, A.A., and Oznobishchev, S.K. (2010) *Strategic Stability after the Cold War*. Moscow: Institute of World Economy and International Relations. Available from: <https://docplayer.net/21467197-Strategic-stability-after-the-cold-war.html> [accessed 17 August 2019].
- Azamatova A.B. and Balpanova N.A. (2017) Kazakhstan's cyber shield – a priority vector of implementation of the national security of the republic of Kazakhstan. *Bulletin of Abay Kazakh National Pedagogical University*. Available from: <https://articlekz.com/en/article/18494> [accessed 22 August 2019].
- Bird, G. (2017) Statement at the UN First Committee. A/C.1/72/PV.3.
- Boyd, J. (1976) Destruction and creation. Presentation. Available from www.goalsys.com/books/documents/destruction_and_creation.pdf [accessed 17 August 2019].
- Broeders, D. (2015) *The Public Core of the Internet: An International Agenda for Internet Governance*. The Hague, The Netherlands Scientific Council for Government Policy.
- Bull, H. (2002) *The Anarchical Society*. New York, Palgrave.
- Clarke, R.A. and Knake, R. (2019) The internet freedom league. How to push back against the authoritarian assault on the web. *Foreign Affairs*. 98(5): 184–192.
- Cleobury, S. (2017) Statement at the UN First Committee. A/C.1/72/PV.20.
- Deutsch, K.W. and Singer, J.D. (1964) Multipolar power systems and international stability. *World Politics*. 16(3): 390–406.
- Department of State, International Security Advisory Board (US) (2014) *Report on A Framework for International Cyber Stability*.
- Dowding, K.M. and Kimber, R. (1983) The meaning and use of 'political stability'. *European Journal of Political Research*. 11: 229–243.
- European Commission (2008) Directive 2008/114/EC (8 December).
- Gaddis, J.L. (2018) *On Grand Strategy*. New York, Allen Lane.
- Gerson, M.S. (2013) The origins of strategic stability: The United States and the fear of surprise attack. In Colby, E.A. and Gerson, M.S. (eds), *Strategic Stability*. Carlisle, Strategic Studies Institute, pp. 3–12.
- Hasani, E. (2002) Reflections on weak states and other sources of international (in)stability. Available from: www.bundesheer.at/pdf_pool/publikationen/hasa02.pdf [accessed 17 August 2019].
- Hurwitz, L. (1973) An index of political stability: A methodological note. *Comparative Political Studies*. 4: 41–68.
- Kazi, F.M. (2017) Statement at the UN First Committee. A/C.1/72/PV.21. Available from: <https://undocs.org/A/C.1/72/PV.21> [accessed 17 August 2019].

- Kerttunen, M. (2018) Policy of consequences as seen through social sciences. *Temple Journal of International and Comparative Law*. 32(2): 71–84.
- Kerttunen, M. (2019) National cyber security strategies: A commitment to development. Blog. Available from: <https://blog.apnic.net/2019/04/04/national-cybersecurity-strategies-commitment-to-development/> [accessed 17 August 2019].
- Kerttunen, M. and Tikk, E. (2019) *Strategically Normative. Norms and Principles in National Cybersecurity Strategies*. Paris, EU ISS.
- Krisnamurthi (2017) Statement at the UN First Committee. A/C.1/72/PV.2. Available from: <https://undocs.org/A/C.1/72/PV.2> [accessed 17 August 2019].
- Körömi, J. (2017) Statement at the UN First Committee. Available from: <https://undocs.org/A/C.1/72/PV.19> [accessed 17 August 2019].
- Libicki, M. (2012) *Crisis and Escalation in Cyberspace*. Santa Monica, RAND Corporation.
- Milner, H.V. (1998) International political economy: Beyond hegemonic stability. *Foreign Policy* 110: 112–123.
- Ministry of Foreign Affairs of the People's Republic of China (CN MFA) (2017) *International Strategy of Cooperation on Cyberspace*.
- Ogilvy-White, T. (ed.) (2011) *On Nuclear Deterrence. The Correspondence of Sir Michael Quinlan*. London, International Institute for Strategic Studies.
- Republic of Kazakhstan (KZ) (2011) On the Concept of Information Security of the Republic of Kazakhstan until 2016. Degree no. 174 (14 November)
- Ristolainen, M. (2017) Should 'RuNet 2020' be taken seriously? Contradictory views about cybersecurity between Russia and the West. *16th European Conference on Cyber Warfare and Security*, Dublin, 29–30 June 2017. In Kukkola, J., Ristolainen, M., and Nikkarila, J.-P. *Game Changer. Structural Transformation of Cyberspace*. Riihimäki, Finnish Defence Research Agency.
- Romashkina, N.P. and Zagorskii, A.V. (2016) *Information Security Threats During Crises and Conflicts of the XXI Century*. Moscow, Primakov Institute of World Economy and International Relations.
- Rose, F.A. (2014) Strategic Stability in East Asia. Remarks at The Johns Hopkins–Nanjing Center for Chinese and American Studies. Nanjing, China (8 December). Available from: <https://china.usc.edu/frank-rose-strategic-stability-east-asia-dec-8-2014> [accessed 17 August 2019].
- Russia Today (RT) (2019) Russia can be unplugged from World Wide Web, but it's not quite ready – co-founder of Kaspersky Lab. (1 March) Available from: <https://www.rt.com/russia/452660-internet-draft-law-attack/> [accessed 17 August 2019].
- Sagan, S.D. and Waltz, K. (2003) *The Spread of Nuclear Weapons. A Debate Renewed*. New York, W.W. Norton, 2003.
- Schelling, T.C. (1958) *Surprise Attack and Disarmament*. Santa Monica, RAND.
- Schelling, T.C. (1960) *The Strategy of Conflict*. Cambridge, Harvard University Press.
- Schelling, T.C. (2013) Foreword. In Colby, E.A. and Gerson, M.S. (eds) (2013) *Strategic Stability*. Carlisle, Strategic Studies Institute.
- Streltsov, A. and Smirnov, A. (2017) Russian–American Cooperation in the Sphere of International Information Security: Suggestions Regarding Priority Areas. *International Affairs* (Moscow).
- Sullivan, J. (2019) Yes, America can still lead the world. *The Atlantic* (January/February).
- The Nation* (2016) Rice prices in Laos stable despite slump in Thailand. *Vientiane* (4 November).
- The President of Russian Federation (RU) (2000, 2008, and 2016) *Information Security Doctrine of the Russian Federation*.
- The White House (US) (2011) *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*. (May 2011).
- The White House (US) (2013) U.S.–Russian Cooperation on Information and Communications Technology Security. (17 June 2013). Available from: <https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol> [accessed 17 August 2019].
- The White House (US) (2018) *National Cyber Strategy of the United States of America* (September).
- United Nations General Assembly (UNGA) (1981) Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States. A/RES/36/103 (9 December).
- United Nations General Assembly (UNGA) (1998) Letter dated 23 September 1998 from the Minister for Foreign Affairs of the Russian Federation addressed to the Secretary-General. A/C.1/53/3 (30 September).

- United Nations General Assembly (UNGA) (2015) 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. A/69/723 (13 January).
- United Nations General Assembly (UNGA) (2018) A/73/27 (8 November).
- United Nations Secretary-General (UNS-G) (1992) *An Agenda for Peace*. A-47-277 S-24111 Available from: <https://digitallibrary.un.org/record/144858> [accessed 17 August 2019].
- United Nations Secretary-General (UNS-G) (2018) *UN Secretary-General's Strategy on New Technologies* (September). Available from: www.un.org/en/newtechnologies/ [accessed 17 August 2019].
- United Nations Security Council (UNSC) (1992) *Note by the President of the Security Council*. S/23500. Available from: <https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/PKO%20S%2023500.pdf> [accessed 17 August 2019].
- United Nations Security Council (UNSC) (2004–2007) *Repertoire of the Practice of the Security Council*. Available from: <https://www.un.org/securitycouncil/content/repertoire/structure> [accessed 17 August 2019].
- United Nations Security Council (UNSC) (2017) S/RES/2341 (13 February).
- Wohlstetter, A. (1958) The delicate balance of terror. RAND P-1472. Available from: <http://www.rand.org/publications/classics/wohlstetter/P1472/P1472.htm> [accessed 17 August 2019].
- Wohlstetter, A. (1959) The delicate balance of terror. *Foreign Affairs*. 37(2): 211–234.
- Zhuang Rongwen (2018) Scientifically understanding the natural laws of online communication, striving to boost the level of internet use and network governance. *Quishi* (21 September). Available from: www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-top-internet-official-lays-out-agenda-for-party-control-online/ [accessed 17 August 2019].

5

IN SEARCH OF HUMAN RIGHTS IN MULTILATERAL CYBERSECURITY DIALOGUES

Allison Pytlak

Introduction

Cybersecurity has come to eclipse the interest and attention of policymakers and the general public alike. Yet despite a stated interest from most stakeholders in preventing mass harm through malicious use of information and communications technologies (ICTs), actual consideration of possible humanitarian impact and human rights violations in particular has not been a significant component of multilateral dialogues on international cybersecurity. The human rights community has mobilized in multiple ways to protect human rights and fundamental freedoms online, yet these efforts remain largely disconnected from the parallel efforts of governments to develop behavioural norms that would govern their actions in cyberspace. Much of that dialogue is occurring within multilateral bodies that take a traditionally state-centric approach to security.

This chapter explores how, in the context of international peace and security, the question of human rights is largely overlooked in multilateral discussions of cybersecurity. It first outlines what is meant by human rights in relation to digital technologies and present the significant body of work that exists to protect these rights as undertaken by both United Nations (UN) entities, states, and civil society. By examining primary documents such as government statements alongside relevant UN resolutions and reports, the chapter next demonstrates how human rights are largely overlooked in relevant peace and security fora that address ICTs. Finally, it seeks to illustrate the benefits of better incorporating human rights and humanitarian perspectives into peace and security-based discussions of cybersecurity by looking at what this has meant in the context of other hard security issues, such as regulating the international arms trade and banning nuclear weapons. The chapter concludes with some procedural recommendations on how to better integrate these two approaches going forward.

The human rights landscape

Human rights in international relations

The concept of human rights has come to be widely understood across the globe, even if receptiveness and adherence is not universal. The creation of the Internet and related digital

networks and platforms has necessitated an examination of how those rights apply to individuals in how their use of, and ability to access, those mediums.

In the offline world, human rights are the fundamental freedoms enjoyed by and guaranteed to individuals by custom or international agreement (United Nations, n.d.). While the concept has a long theoretical history, accompanied by sometimes irregular application in national practice, it was not until 1945 that human rights came to be recognized in international law (Forsythe, 2006). The United Nations Charter adopted that year, 'reaffirmed faith in fundamental human rights, and dignity and worth of the human person' and committed all UN member states to promote 'universal respect for, and observance of, human rights and fundamental freedoms for all without distinction as to race, sex, language, or religion' (United Nations, 1945). This set into motion a process that led to the adoption to the 1948 Universal Declaration of Human Rights (UDHR), generally agreed to be the foundation of international human rights law (IHRL). It represents the universal recognition that basic rights and fundamental freedoms are inherent to all human beings, inalienable and equally applicable to everyone, and that every one of us is born free and equal in dignity and rights. The recognition of human rights, seen by some as a precursor to the human security concept, represents a significant conceptual shift by placing greater weight on the rights of individuals and their security, as persons, than to the security of the nation-state (Forsythe, 2006).

Human rights law has been defined over the ensuing decades through international conventions, treaties, and organisations. There are nine core human rights instruments (UN Office of the High Commissioner for Human Rights, 2019). Each of these instruments is monitored by a committee of experts and some are supplemented by optional protocols dealing with specific concerns. Responsibility for the implementation of human rights laws and obligations rests with national governments however, and the gap between what is said and done at the United Nations versus what occurs in national practice is not insignificant.

The evolution of digital human rights

The advent of the Internet and subsequent increased reliance on digital technologies for everything from banking to personal communications over the last fifteen years has presented new challenges for the application of human rights law. While digital networks and mediums offer the possibility of improved monitoring and knowledge-sharing, they are themselves sometimes used as a tool in human rights repression or as a space in which abuses conducted offline can be exacerbated (Donahoe, 2014).

The rise in popularity of social media platforms such as Facebook, YouTube, and Twitter catalysed efforts to both understand and better articulate the applicability of human rights law online. This has included both the rights that individuals have in how they use ICTs and what they choose to post or make public, but also to protect from citizens from having ICTs or their personal data used against them. The early use of such platforms and their messaging services by citizen groups to organize for change, generated interest among scholars to understand the potential of these technologies to aid in political revolution (Shirky, 2011). This was especially true in the context of the Arab Spring but in other places such as Moldova and Iran as well (Safranek, 2012).

Such actions generated backlash from authorities, such as through the implementation of measures by national governments to gain control of the access and use of social media networks for political action. Practices of 'cyber repression' have continued if not expanded over

the last decade, aided in part by technological evolution. Increasingly sophisticated spyware has made it possible for governments or other actors to obtain sensitive information about media agencies, human rights defenders, and other civil society organizations (Citizen Lab, n.d.). From Venezuela to Zimbabwe, China to Cameroon, there are multiple examples of Internet shutdowns, content removal from websites, and censorship including through offline punishment and intimidation practices (Valeriano & Pytlak, 2017) (Internet sans frontieres, 2017) (Global Partners Digital, 2018).

Around the same time as social media began to be used for political organising and expression, the Edward Snowden revelations about United States' (US) surveillance activities underscored the fact that Western democracies are not immune to online human rights abuses either (Dencik & Cable, 2017). Until then, censorship and surveillance practices could be dismissed as by-products of autocratic or authoritarian regimes, but the revelations showed this was not only inaccurate but highlighted the dangers of digitization, data collection, and the collapse of the online/offline divide (Donahoe, 2016). The revelations and ensuing debate further underscored how ICTs and cybersecurity activities can be co-opted by the agendas of counterterrorism or countering extremism online in ways detrimental to personal rights and freedoms. Balancing the justifiable need to prevent ICTs from being misused to incite or promote violence, with human rights, often represents political, normative, and legislative challenges for states (Council on Foreign Relations, 2016).

Responses to digital human rights abuse

Incidents such as those described above have made it clear to many in the international community that it is necessary to adapt and apply existing human rights law for the digital ecosystem. Some approaches have necessarily focused in on single specific human rights concerns, such as the right to freedom of expression, as protected by Article 19 of the UDHR and of the International Covenant on Civil and Political Rights (1966). The human rights to privacy and assembly are also frequently at risk in a digital context. The right to privacy is guaranteed by Article 17 of the International Covenant on Civil and Political Rights (1966). Article 15 of the International Covenant on Economic, Social and Cultural Rights (1966) protects the right of everyone to “enjoy the benefits of scientific progress and its applications” which can be interpreted to include the right to use the Internet. A recent UN Human Rights Council (HRC) resolution took focus on women's human rights as threatened by targeted online activities like revenge porn and cyberstalking (UN HRC, 2018).

The Association for Progressive Communications published in 2006 an Internet Rights Charter which became a foundational document for efforts in this area, particularly among civil society organizations (Association for Progressive Communications, 2006). Organized across seven thematic areas, the APC Charter was premised on the belief that ability to share information and communicate freely using the Internet is vital to the ‘realisation of human rights’ as enshrined core human rights instruments. It was followed up by a Charter of Human Rights and Principles for the Internet developed by the Internet Rights and Principles Dynamic Coalition (Internet Rights and Principles Dynamic Coalition, 2009).

The UN Human Rights Council, a UN body comprised of 47 UN member states with foremost authority over human rights issues, has now passed multiple resolutions relevant to the Internet or digital contexts more broadly. The first, adopted in 2012, was considered landmark for not only being the first on the subject but also for its affirmation that ‘the human rights people enjoy offline, also apply online’ (UN Human Rights Council, 2012).

The resolution built on a 2011 report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (La Rue, 2011).

The right to privacy in the digital age has also been taken up by the UNGA Third Committee. In December 2013, the United Nations General Assembly (UNGA) adopted resolution 68/167 ‘The Right to Privacy in the Digital Age’ which called on all states to review their procedures, practices, and legislation related to communications surveillance, interception, and collection of personal data. It further emphasized the need for states to ensure the full and effective implementation of their obligations under international human rights law. The resolution was the foundation for a 2014 report of the Office of the United Nations High Commissioner for Human Rights on the same subject, for which the views of multiple stakeholders were solicited (UN High Commissioner for Human Rights, 2014) and for a follow-up resolution in 2015.

The UN Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression recently issued a report focused on the obligations of states and companies, by aiming to find user-centric and human rights law-aligned approaches to content policy-making, transparency, due process, and governance (Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 2018).

Beyond the United Nations are the day-to-day advocacy and other initiatives of non-governmental organizations and individual human rights defenders such as groups like APC, Human Rights Watch, Amnesty International, Privacy International, Global Partners Digital, Electronic Frontier Foundation, the Freedom Online Coalition, and Citizen Lab, among others. Technologists have added to this work by developing applications and software to prevent intrusions, detect censorship, or enable anonymity online (Open Observatory for Network Interference, 2018). It is also worth noting that ICTs are increasingly being used in the pursuit and defence of human rights, to capture violations and facilitate sharing. (Amnesty International, n.d.).

It is evident that there is an ever-growing community of practice within the broader human rights movement that is focusing on protecting human rights in a digital context. This represents a very different approach to how ICTs are discussed within the peace and security community, as the next section will demonstrate.

Multilateral discussion on ICTs in the context of peace and security

The United Nations has been considering ‘developments in the field of information and telecommunications in the context of international security’ since 1998. The locus of discussion has been within Groups of Governmental Experts (GGEs) on ICTs established by the UNGA as of 2004. The UNGA’s First Committee on International Security and Disarmament – the body in which the resolutions mandating the GGEs originate – has over time become a space in which stakeholders outline their views or present expertise on this subject. The UN Secretary-General (UNSG) has issued multiple reports on the subject of ICTs. The work within the UN is supplemented by an external patchwork of global and regional meetings for various stakeholders. Some of these fora have come to play an increasingly important role given stalemate and politicization within the UN system (Meyer, 2018).

While taking a brief look at these external fora, this section will largely focus on how international cybersecurity and ICTs are approached within UN peace and security bodies, and then examine relevant documentation to demonstrate the militarized approach adopted by these entities, in which human rights or humanitarian impacts are either marginalized or overlooked.

ICTs in the UN peace and security framework

In the UN context, General Assembly resolutions relating to issues of disarmament or security are first presented, debated, and tabled for adoption in the UNGA's First Committee (United Nations, n.d.).

The Russian Federation introduced the first draft resolution on the subject of in the context of international security in 1998 (UNGA First Committee, 1998). It had four operative paragraphs, including a call to member states to inform the UNSG of their views and assessments on four key questions relating to information security. These formed the basis of the annual reports that UN Secretary-Generals have published since 1999.

The 2002 resolution called for the establishment of the first GGE on ICTs, prompted in part by reluctance from some countries to fully engage in this subject in First Committee (Tikk & Kerttunen, 2018). Five GGEs have since been convened, each meeting either in Geneva or New York four times over a two-year cycle (UN Office for Disarmament Affairs, 2019). Their sizes have ranged from 15–25 states (UN Office for Disarmament Affairs, 2019). Each Group seeks to agree by consensus a report of its proceedings, that may include conclusions and recommendations, and which are returned to the wider UN membership for adoption. This has had varying levels of success.

Since inception, the GGEs have suffered from an inherent sense of mistrust among some of their key members and divergent views about definitions and basic approaches to information security. Other areas of contention have included GGE mandates as well as the broader role of the UN and the First Committee with respect to international information security challenges (Tikk & Kerttunen, 2018).

Over time changes in the international landscape, including the first real known cases of malicious use of ICTs amongst and between states led to greater productivity and agreements among GGE members (Tikk-Ringas, 2012). The 2012–2013 report was welcomed for its breakthrough statement that international law is applicable to cyberspace, yet was simultaneously tempered by a reaffirmation of state sovereignty in the conduct of ICT-related activities, and protection of infrastructure (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013). The somewhat vague and contradictory nature of the 2013 statement was noted by some as indicative of disagreement yet to come. The 2015 report was lauded for setting out eleven recommendations for voluntary and non-binding norms, rules, or principles for state behaviour, confidence-building measures, international cooperation and capacity building, and positive recommendations (UN Office for Disarmament Affairs, 2019). Less reported on, but relevant to this chapter, was the recommendation in paragraph 13(e) that states must comply with obligations to respect and protect human rights and fundamental freedoms (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015). This recommendation was voluntary in nature and, as in 2013, balanced out by the reaffirmation of state sovereignty in the applicability of international law in paragraph 26, in an effort to obtain agreement from all states in the Group (Sander, 2017).

When progress broke down in the 2016–2017 Group, reportedly over the issue of the applicability of international law, including international humanitarian law (IHL) and IHRL, it was perhaps not surprising. The United States and many European countries participating in the Group had sought greater specificity on this point in the Group's planned report. The US in particular sought a package of references to international law, IHL, as well as to countermeasures and the right to self-defence as outlined by Article 51 of the UN Charter

(US Department of State, 2019). Their efforts were resisted by others, notably China, Russia, and Cuba, who argued that recognition of IHL and Article 51 in particular would constitute a legitimisation of cyber conflict (Tikk & Kerttunen, 2018). It is important to read between the lines and understand that textual suggestions on all sides were underpinned by political motivations, and the nature of practical actions already being undertaken by states in cyberspace, both internationally and domestically. The disagreement also demonstrated the wide divergence of views and approaches to ICTs and international cybersecurity (Tikk & Kerttunen, 2018).

The Russian Federation has continued to be the main sponsor of UNGA First Committee resolutions on ICTs in the context of international security, a resolution that has always been relatively straightforward and similar in content from year to year, while also reflecting outputs from the GGEs and other developments. In 2018, it struck a difference course by introducing a resolution with some new and controversial elements, prompting the United States to table its own. (Grigsby, 2018). Despite revisions, intense politicisation at the 2018 First Committee prevented compromise (Pytlak, 2018). Both resolutions were adopted, and the General Assembly has established both a new GGE and an Open-Ended Working Group (OEWG) to continue ICT discussions for the period of 2019–2021 and 2019–2020 respectively (UN Office for Disarmament Affairs, 2019).

Beyond UNGA structures, international cybersecurity has been taken up through an Arria-formula meeting of the UN Security Council in December 2016. The International Telecommunications Union (ITU) has been an active part of the UN community in the context of ICTs and cybersecurity as the UN's specialized agency that provides support to member states to develop technical standards and improve connectivity.

The (under) representation of human rights within international cybersecurity fora

Across these various fora, how large of a role do human rights play? Evidence suggests that it is a marginal one at best; a consequence of treating ICTs or cybersecurity within disarmament and security frameworks is that the subject has come to be treated as a hard security issue. This means that 'cybersecurity' is more about 'national cybersecurity' and the protection of the cyber-physical environment than about preventing civilian harm or protecting rights.

a) UNGA resolutions

Human rights only began to be referenced in these resolutions as of 2013 through the inclusion of a preambular paragraph (PP): 'Noting the importance of respect for human rights and fundamental freedoms in the use of information and communications technologies.' Preambular paragraphs provide a framing for a resolution, and do not set out any actions. They can be a space to reference other UN or legal documents that relate to the content of the resolution but to date, none of the UNGA First Committee resolutions on ICTs have made a reference to UNGA Third Committee resolutions on human rights and ICTs, or documents produced by the Human Rights Council or relevant Special Rapporteurs, despite there being a clear overlap between when human rights began to emerge in the First Committee and GGE reports as a cyber issue, and when the Third Committee and Human Rights Council began to pass relevant resolutions on digital technologies.

The Russian Federation-sponsored 2018 resolution includes the first operative paragraph (OP) reference to human rights. This follows preambular references welcoming the findings

of the 2015 report with respect to human rights and underline the importance of respecting human rights and fundamental freedoms. It is balanced by another preambular reference to UNGA Resolution A/RES/36/103 which also sets out important human rights recognitions in relation to access to and use of information, yet reaffirms state sovereignty and jurisdiction in this regard, and the principle non-intervention (UN General Assembly, 1981). The OP articulates that: ‘States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 of 5 July 2012 and 26/13 of 26 June 2014 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 of 18 December 2013 and 69/166 of 18 December 2014 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.’ The United States-sponsored resolution of the same year includes a preambular reference only.

b) GGE reports

The inclusion of human rights in two of three reports of the UN GGEs on ICTs have already been touched on, but it is useful to have a better understanding of their contents.

The 2011–2013 Group’s report was minimal in this area but is important nonetheless for being the first such human rights reference in a GGE report. These reports are agreed by consensus – which in the UN system means unanimity – and therefore in this instance means that states not generally supportive of human rights were willing to recognize 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’ (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013).

The report of the 2014–2015 Group called on states to respect HRC resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, and ‘to guarantee full respect for human rights, including the right to freedom of expression’ (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015). Second, the report reaffirmed that human rights, among other principles, was identified as of ‘central importance in the consideration of the application of international law to state use of ICTs.’ Finally, it urged the UN to play a leading role in dialogue promotion – but to not duplicate the work of other fora discussing other human rights and Internet governance aspects of ICTs.

c) National reports to the UNSG, and UNSG reports

A review of national submissions available online and cited in the UNSG reports and addendums shows that over time, the volume of submissions has increased yet references to human rights have not kept pace. National submissions are either included in UNSG reports or if too lengthy, posted in full online by the UN Office of Disarmament Affairs (UNODA). It is important to bear in mind that these submissions are irregular and that reporting rates in general are quite low. The first such references were made by the Netherlands and the US in 2011 (UN Secretary-General, 2011).

In 2014 nine of 16 submissions had a human rights reference (Australia, Austria, Canada, France, Germany, Spain, Sweden, Switzerland, and the United Kingdom) (UN Office of Disarmament Affairs, 2019).

Austria, Canada, and Spain reaffirmed the importance of protecting human rights online; Australia and Switzerland spoke to the applicability of IHRL in cyberspace. France, as the UK did in a subsequent year, took a somewhat more political direction in its submission by clarifying its understanding of ‘information security’ (UN Secretary-General, 2016).

The overall number of submissions rose to 24 in 2017 yet only seven states referred to human rights or human rights law. Canada and the United Kingdom (UK) were the most expansive on this subject; others included a more general statement about the protection of human rights online. Canada’s statement reinforced the role that ICTs can play in advancing human rights, and also described its efforts to bringing a ‘human rights framing to cybersecurity issues’ as part of its work in the Freedom Online Coalition (Government of Canada, 2017). It further noted the applicability of IHRL to cyberspace, as did the UK with specific mention of the UDHR and the International Covenant on Civil and Political Rights (Foreign and Commonwealth Office, United Kingdom of Great Britain and Northern Ireland, 2017).

d) UNGA First Committee

As noted earlier in this chapter, the UNGA First Committee has overtime become a place where states engage in this topic more frequently. Cybersecurity or ICTs (they two terms are often used interchangeably there) are referenced either briefly as part of the general statements delivered at the opening of the UN First Committee sessions each year, or in greater depth during a thematic segment on ‘Other disarmament measures’. Findings in this subsection were obtained by a review of all available statements from the 2015–2018 UNGA First Committee as posted on the website of Reaching Critical Will, which conducts civil society monitoring and analysis of the First Committee. The author reviewed statements delivered as part of the ‘Other disarmament measures’ section in these years.

In 2017, the year in which the GGE did not produce a consensus report amid significant disagreement, around 19 delegations referenced cyber/ICTs in this same segment and 11 delegations (the EU, Switzerland, Paraguay, Brazil, Netherlands, UK, Germany, Zambia, Russian Federation, Austria, and Australia) mentioned human rights (Reaching Critical Will-WILPF, 2015–2018). Many of these were made in the context of a re-affirmation of the applicability of international law, including human rights law, to cyberspace – which had been a primary area of disagreement. In 2018, in which there were two resolutions tabled for paths forward on ICTs in the UN, around 12 delegations referenced cyber/ICTs during the ‘Other’ thematic segment; only five spoke of human rights or IHRL. These included the European Union, the Netherlands, Mexico, UK, Iran and a joint statement from six countries, delivered by Canada. In earlier years there were far fewer human rights references; three in 2016 and four in 2014.

e) Beyond the UN

As noted earlier in this chapter, politicisation and frustration at the slow pace of progress on UN-based ICT fora are sparking action elsewhere. France initiated its ‘Paris Call for Trust and Security in Cyberspace’ in November 2018 (France Diplomatie, 2018). The Call makes note of the applicability of human rights law to cyberspace. Also in 2018 the Global Commission on the Stability of Cyberspace (GCSC) outlined six new global norms to help promote the peaceful use of cyberspace – which do not once reference human rights, civilian impacts, or humanitarian harm caused by malicious government cyber operations (Global

Commission on the Stability of Cyberspace, 2018). Proposals have also come from the private sector, notably Microsoft's suggestion for digital Geneva Convention (Microsoft, 2017) and leadership in the development of the Tech Accords, now supported by dozens of technology firms. The documents do not explicitly speak to human rights but some have noted that certain of their provisions have potential (Kaspar, 2018).

This brief survey of national statements and UN documents underscores that human rights and human rights law are not a priority when states discuss international cybersecurity. Only a small percentage of states express such concerns, and those are usually only a small component of a broader package of stated priorities and areas for further discussion. Of course, simply increasing the number of passing references in a document or statement should not be an end goal in itself. In fact, recognizing developments in the human rights community is an important part of integrating a human rights perspective, states must go further to more explicitly apply human rights law to their international cyber activities. The next section of this chapter will identify the benefits in doing so, followed by recommendations.

Challenges and benefits to promoting human rights perspectives in international cybersecurity

Given the information presented above, two key questions emerge: why are human rights such a small part of international cybersecurity dialogues, and why is it important to overcome that?

There are multiple possible reasons why human rights have not been a bigger concern for states when considering international cybersecurity. A first may relate to the structure of the United Nations itself and how it separates and silos issues. There are clear lines of division across the system: between the UN Security Council and the UN General Assembly; across the GA's six committees; and between agencies and departments. There are obvious division of labour benefits to this approach but it does inhibit policy coherence. The ITU could potentially have a role to play in streamlining the proposals and guidance coming out of the many parts of the UN.

Another possibility is that states do not *want* to connect the two or integrate human rights perspectives. The concept of human rights is not embraced everywhere and is still viewed by some states and individuals as a projection of Western, liberal-democratic values. Differences linger over how states view the way in which the UNGA First Committee and the GGEs approach the ICT issue, and even what is meant by cyber, information security, and ICTs.

Moreover, several countries who advocate for human rights perspectives are not necessarily practicing what they preach, online as well as offline. Evidence continues emerge about American and British surveillance technology sales to so-called authoritarian states as well as about the use of spyware in their own countries and in France (Franceschi-Bicchierai, 2018) as a few examples. Australia has spoken in favour of the online protection of human rights yet in late 2018 rushed through its parliament controversial and far-reaching legislation on encryption which experts say pose a threat to cybersecurity, privacy, freedom of expression and human rights (Brookes, 2019). Closer discussion about digital human rights within security fora could expose these double standards and weaken the pro-human rights arguments of advocates.

Yet, possibly one of the largest challenges is an overall lack of understanding about what a human rights perspective in international cybersecurity means. It's one thing to acknowledge

relevant HRC resolutions or to affirm the applicability of human rights law online – but what do human rights mean in the context of state-to-state cyber operations and behaviour and why do they matter to international cybersecurity?

As civil society groups noted in a 2018 joint statement to the UNGA First Committee, ‘Another [way to challenge militarization] is to put human rights and the humanitarian impact of misused digital technologies at the centre of the discussion. Treating cyberspace and related actions in a sanitised, faceless way risks institutionalising and taking for granted the broader idea of cyber conflict’ (Multiple authors, 2018).

Current approaches to international cybersecurity place the nation state as the beneficiary of norms, protections, or laws from any perceived attack on its interests or security. As just one example, consider that when foreign hackers are tried for cyber espionage it is for espionage against governments or the private sector, not for actions undertaken against individual citizens (Deibert, 2018).

It can be useful to look how the inclusion of human rights or humanitarian perspectives within other security issues contributed to changing the discourse from one oriented toward conflict or militarism, to a peace-orientation in which preventive measures are prioritized over largely remedial and operative responses.

The 2013 Arms Trade Treaty (ATT) was adopted in response to widespread concern about the humanitarian and human rights impact of the unregulated trade in conventional arms. Under the ATT, an arms transfer should not be authorized if the state party has knowledge that the arms or items would be used in the commission of genocide, crimes against humanity, war crimes or other serious violations of both international humanitarian law and international human rights law (UN General Assembly, 2013). The ATT is regarded as ‘pioneering’ (MacFarquhar, 2013) for putting human rights at the centre of an international weapons control agreement.

The historic accomplishment was hard fought, involving seven years of negotiation after nearly a decade of awareness-raising and advocacy. Campaigning for controls necessitated a message of ‘people before profit’ along with lifting up the experiences of survivors of armed violence and demonstrating through research the links between the international arms trade, human rights abuse including gender-based violence, socio-economic development, corruption, and transparency (Amnesty International, n.d.).

There are still states who do not accept the human rights premise of the ATT. At the time of its adoption, states such as Bolivia, Cuba, and Nicaragua said they had abstained because the human rights criteria could be abused to create political pressure (MacFarquhar, 2013). The overwhelming level of support for the Treaty – it has 100 states parties and 35 signatories – demonstrates however that there is now broad acceptance of a humanitarian and human rights approach to regulating international arms transfers.

The 2017 adoption of the Treaty on the Prohibition of Nuclear Weapons (TPNW) is perhaps even more ground-breaking. Nuclear weapons were the only weapons of mass destruction not subject to a categorical ban, despite their catastrophic humanitarian consequences. The achievement of the Treaty required a dramatic reframing of nuclear weapons and concepts of security used in earlier arms control agreements (Acheson, 2018).

The campaign for the TPNW emerged from the Humanitarian Initiative, a years-long effort led by civil society through the International Campaign to Abolish Nuclear Weapons (ICAN), the ICRC, and a core group of non-nuclear weapon states advocating that the ‘catastrophic, persistent effects of nuclear weapons on our health, societies and the environment must be at the centre of all public and diplomatic discussions about nuclear disarmament and

non-proliferation’ (International Campaign to Abolish Nuclear Weapons, 2018). ICAN was awarded the 2017 Nobel Peace Prize for its work in this regard (Heldin, 2017), following the Treaty’s adoption in 2017.

An important difference between those treaties and cybersecurity issues of course is that they regulate or prohibit tangible weapons whereas there is not a universally accepted definition of a ‘cyber weapon’ (New America Foundation, 2019). Yet these examples are instructive in demonstrating that narratives and discourse can be changed, to allow for a fuller incorporation of human rights within otherwise challenging and politically-sensitive security issues.

Recommendations and conclusions

How then, to advance a human rights perspective within international cybersecurity dialogues?

One first step is to encourage research that brings a human face and dimension to analysis and discussion about cyberattacks and operations. There is ample testimony of domestic repression collected by digital human rights groups that has not been well-examined within peace and security bodies, and more needs to be done in the context of highlighting the costs of interstate cyber operations and global cyber security. Information resources like these were transformative in the campaigns for the ATT and TPNW. While the specific impacts and human costs may be different in this sphere, but are no less important to illustrate.

Yet, this must be accompanied by opportunities to share such information with states in a meaningful way, and for states to set aside time for discussion about the human rights dimension instead of treating it as a fringe concern. More openness and transparency within international peace and security bodies discussing cyber security is a must, and a part of that is engaging with other, non-governmental stakeholders. The GGEs had been completely closed; the only opportunity for non-governmental entities of any stripe to engage in this issue at the UN was during the First Committee, and that has been minimal, typically consisting of perhaps one or two side events each year, an annual joint NGO intervention, and written analysis. The new OEWG and proliferation of non-UN norm development platforms bring the possibility of change but it will be important to avoid tokenistic displays of openness. If new entities are approached from a rights-based and stakeholder perspective at the outset there is greater potential to shift the narrative and include human rights in their design.

States must move away from approaching international cybersecurity through a traditional arms control and disarmament lens, and the state-centric security concepts and tools that come with it. Nuclear deterrence has been used for decades as a way for a powerful few countries to justify the development of vast and expensive arsenals of catastrophic and indiscriminate weapons; its re-emergence as ‘cyber deterrence’ is not only conceptually awkward but will inevitably foster responses that are similarly hyper-militarized. Understanding cybersecurity on its own terms, and where human rights fit into that unique landscape, is crucial to developing effective policy responses.

By mapping out the separate digital human rights and international cyber security landscapes this chapter has shown that despite wide divide there is potential for integration. Lessons may be taken from the experiences of hard security issues, or perhaps a new path will be taken. Regardless, it’s past time that human rights play a more integral role in multilateral dialogues on international cybersecurity.

References

- Acheson, R. (2018). *How Prohibiting Nuclear Weapons Changed the World*. New York: The Nation.
- Amnesty International. (n.d.). *An Arms Trade Treaty: Minimum standards to control the international arms trade*. Retrieved from <https://www.amnesty.org/download/Documents/100000/act300022003en.pdf>
- Amnesty International. (n.d.). *Citizen Evidence Lab*. Retrieved from <https://citizenevidence.org/>
- Association for Progressive Communications. (2006). Internet Rights Charter.
- Brookes, J. (2019). *Tech Giants And Civil Liberties Groups Unite To Challenge Australian Encryption Laws*. Retrieved from <https://which-50.com/tech-giants-and-civil-liberties-group-unite-to-challenge-australian-encryption-laws/>
- Citizen Lab. (n.d.). *Spyware*. Retrieved February 2019, from <https://citizenlab.ca/tag/spyware/>
- Council on Foreign Relations. (2016, February 4). *UN Counter-Terrorism Committee Tackles Terrorist Use of the Internet and Social Media*. Retrieved March 19, 2019, from <https://www.cfr.org/blog/un-counter-terrorism-committee-tackles-terrorist-use-internet-and-social-media>
- Cyber. (2018; 2017; 2016). *First Committee Monitor*. Reaching Critical Will/WILPF.
- Deibert, R. J. (2018). Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs*, 32(4), 411–424.
- Dencik, L., & Cable, J. (2017). The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks. *International Journal of Communication*, 11, 763–781.
- Donahoe, E. (2014). Human Rights in the Digital Age. Just Security.
- Donahoe, E. (2016). So Software Has Eaten the World: What Does It Mean for Human Rights, Security & Governance? Just Security.
- Foreign and Commonwealth Office, United Kingdom of Great Britain and Northern Ireland. (2017). Response to General Assembly resolution 71/28 “Developments in the field of information and telecommunications in the context of international security.”
- Foreign and Commonwealth Office, United Kingdom of Great Britain and Northern Ireland. (n.d.). Response to General Assembly resolution 71/28 “Developments in the field of information and telecommunications in the context of international security. 2017.
- Forsythe, D. (2006). *Human Rights in International Relations*. Cambridge University Press.
- France Diplomatie. (2018). *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*. Retrieved from <https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in>
- Franceschi-Bicchierai, L. (2018). *Cyber Sleuths Find Traces of Infamous iPhone and Android Spyware ‘Pegasus’ in 45 Countries*. Retrieved from https://motherboard.vice.com/en_us/article/bjaz94/nso-group-pegasus-45-countries-map-spyware-citizen-lab
- Global Commission on the Stability of Cyberspace. (2018). *Norm Package Singapore*.
- Global Partners Digital. (2018). The Digest: 2018 in Review.
- Government of Canada. (2017). Developments in the Field of Information and Telecommunications in the Context of International Security.
- Government of Cuba. (2017).
- Government of Ecuador. (2017). Resolucion 71/28 « Desarrollo en el campo de la informacion y las telecomunicaciones en el contexto de la seguridad internacional ».
- Grigsby, A. (2018, October). *Unpacking The Competing Russian and U.S. Cyberspace Resolutions at the United Nations*. Retrieved from <https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutions-united-nations>
- Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2013). *Report*. New York: UN General Assembly.
- Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2015). *Report*. New York: UN General Assembly.
- Heldin, C.-H. (2017). Opening Address: Nobel Prize Award Ceremony. Oslo.
- International Campaign to Abolish Nuclear Weapons. (2018). *The Humanitarian Initiative*. Retrieved from <http://www.icanw.org/campaign/humanitarian-initiative/>
- Internet Rights and Principles Dynamic Coalition. (2009). Charter of Human Rights and Principles for the Internet.

- Internet sans frontieres. (2017). *Internet shutdown in Cameroon is expensive*. Retrieved from <https://internetwithoutborders.org/internet-shutdown-in-cameroon-is-expensive/>
- Karzak, E. (2017, July 31). UN GGE on Cybersecurity: The End of an Era? *The Diplomat*. Retrieved from <https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/>
- Kaspar, L. (2018). Microsoft's Tech Accord – and what it tells us about the cyber state of play. *Global Partners Digital*.
- La Rue, F. (2011). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. Geneva: UN Human Rights Council.
- MacFarquhar, N. (2013). U.N. Treaty Is First Aimed at Regulating Global Arms Sales. *New York: New York Times*.
- Meyer, P. (2018). *Global Cyber Security Norms: A Proliferation Problem?* ICT4Peace.
- Microsoft. (2017). *A Digital Geneva Convention to protect cyberspace*. Retrieved from <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH>
- Multiple authors. (2018, October 17). *Civil society statement on cyber and human security*. Retrieved from http://reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com18/statements/18Oct_Cyber.pdf
- New America Foundation. (2019). *Global Cyber Definitions Database*. Retrieved from <http://cyberdefinitions.newamerica.org/>
- Open Observatory for Network Interference. (2018).
- Pytlak, A. (2018, November 11). Cyber. *First Committee Monitor*, pp. 9–10.
- Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. (2018). Geneva: Office of the United Nations High Commissioner for Human Rights.
- Reaching Critical Will–WILPF. (2015–2018). *UN General Assembly First Committee*. Retrieved March 19, 2019, from <http://reachingcriticalwill.org/disarmament-fora/unga>
- Safranek, R. (2012). *The Emerging Role of Social Media in Political and Regime Change*.
- Sander, B. (2017). 13(e). *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology A Commentary*, 95–168.
- Security Council Report. (2016). *What's in Blue: Open Arria-formula meeting on cybersecurity*. Retrieved from <https://www.whatsinblue.org/2016/11/open-arria-formula-meeting-on-cybersecurity.php#>
- Shirky, C. (2011). The Political Power of Social Media: Technology, the Public Sphere, and Political Change. *Foreign Affairs*, 90(1), 28–41.
- Stockholm International Peace Research Institute. (2017). *SIPRI Arms Transfers Database*. Retrieved from <https://sipri.org/databases/financial-value-global-arms-trade>
- The Human Cost of Cyberattacks* (2018). [Motion Picture].
- Tikk, E., & Kerttunen, M. (2018). *Parabasis: Cyber-diplomacy in Stalemate*. Oslo: Norwegian Institute of International Affairs.
- Tikk-Ringas, E. (2012). *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998–2012*. Geneva: ICT4Peace Foundation.
- UN General Assembly. (1981). Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States. New York: United Nations.
- UN General Assembly. (2013). The Arms Trade Treaty.
- UN General Assembly. (2017). Treaty on the Prohibition of Nuclear Weapons.
- UN High Commissioner for Human Rights. (2014). *The right to privacy in the digital age*. UN Office of the High Commissioner for Human Rights.
- UN Human Rights Council. (2012). The promotion, protection and enjoyment of human rights.
- UN Human Rights Council. (2018). Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts. Geneva.
- UN Institute for Disarmament Research. (2019). *Cyber Policy Portal*. Retrieved from <https://cyberpolicyportal.org/en/>
- UN Office for Disarmament Affairs. (2019). Factsheet: Developments in the field of information and telecommunications in the context of international security. New York: United Nations.
- UN Office of Disarmament Affairs. (2019). Retrieved February 2019, from www.un.org/disarmament/topics/informationsecurity
- UN Office of the High Commissioner for Human Rights. (2019). *Universal Human Rights Instruments*. Retrieved from <https://www.ohchr.org/EN/ProfessionalInterest/Pages/UniversalHumanRightsInstruments.aspx>

- UN Press Service. (2013). *First Committee Speakers Greet Arms Trade Treaty as 'Epoch-Making' Achievement Capable of Restraining Proliferation If Backed by Strict Export Controls*. Retrieved from <https://www.un.org/press/en/2013/gadis3489.doc.htm>
- UN Press Service. (2014). Intense Debate, Close Voting as Gender Identity, Sexual Orientation, Digital-age Privacy Take Centre Stage in Third Committee. New York.
- UN Secretary-General. (2011). *Report of the Secretary-General: Developments in the field of information and telecommunications in the context of international security*. UNGA.
- UN Secretary-General. (2016). *Developments in the field of information and telecommunications in the context of international security*. New York.
- UNGA First Committee. (1998). Developments in the field of information and telecommunications in the context of international security.
- United Nations. (1945). *Universal Declaration of Human Rights*.
- United Nations. (n.d.). *Disarmament and International Security (First Committee)*. Retrieved 2019, from <https://www.un.org/en/ga/first/>
- United Nations. (n.d.). *Human Rights*. Retrieved from <http://www.un.org/en/sections/issues-depth/human-rights/>
- US Department of State. (2019). 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.
- Valeriano, B., & Pytlak, A. (2017). The Frontlines of Cyber Repression: Thailand and the Crop Top King. Niskanen Center.
- Valeriano, B., & Pytlak, A. (2017). The Frontlines of Cyber Repression: The Venezuelan Digital Caudillo. Niskanen Center.

6

INTERNATIONAL GOVERNANCE OF/IN CYBERSPACE

Tang Lan (translated by Nigel Inkster)

With the further development of networks, informationization and intelligentization, cyberspace has become a new carrier, a new platform, and a new channel for conduct in areas including national politics, the economy, and the military; and traditional Internet governance has entered a new stage of cyberspace governance, involving multiple subjects, many topics and complex mechanisms. This transformation has given rise to difficulties in the international governance of cyberspace. Issues such as competition for power between state and non-State actors, the contradiction between the development of a digital economy and political security, and the proliferation of governance challenges brought about by new technologies are all impacting on the ecology of global network governance, and the rebalancing of the forces in this ecology will promote innovation in the way governance develops.

Based on this, promoting the transformation of the international governance system of cyberspace has become a key focus of the international community. Firstly, the development of Internet governance to cyberspace governance is an inevitable trend. Internet governance was first integrated into the global horizon at the 2003 United Nations World Summit on the Information Society (WSIS), in which the Geneva Plan of Action adopted by participating States requested the Secretary-General of the United Nations ‘to set up a working group on Internet governance’ and ‘make proposals for action, as appropriate, on the governance of Internet by 2005’ (#13b). The Plan of Action also gave the Working Group four main tasks, including the development of a working definition of Internet governance, the identification of public policy issues related to it, the formation of consensus on the roles and responsibilities of the various actors and the drafting of the report for consideration at the 2005 session.

But before that, in respect of the allocation of Internet resources, the governance of the Internet framework had begun. Scholars, such as Mueller (2010 and 2017) and Palfrey (2010), usually divide Internet governance into four stages. The precise labels of periods varying, the first, early period of Internet governance can be divided into two: the birth of the Internet between 1970 and 1994 and the 1994–1998 Domain Name System war. As governments and the private sector became aware of the importance of global networks, the centrality of Internet governance soon began to change, and the Internet Corporation for Assigned Names and Numbers (ICANN), established in 1998, was the product of the war. The second stages can be said to be signified by Internet governance making its way onto the diplomatic agenda. The convening of the World Summit on the Information Society in 2003 and 2005 exemplify the

progress. The third is the development and expansion phase (2006–2013) where the international community has embarked on the implementation of the Tunis Agenda and the Tunis Commitment. In particular, the convening of IGF has given rise to the experiment of multi-lateral diplomacy in Internet governance. The fourth stage can be characterized as a reform phase (2013–present). The Snowden incident has raised concerns about Internet governance in relation to privacy and data protection issues, and countries have questioned the US monopoly on key Internet resources, giving further impetus to ICANN's internationalization process.

Internet governance is a complex area. The 2005 United Nations WGIG work report provided the following working definition: 'Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet' (WGIG, 2005, #10). Its concern about the influence of Internet development on various fields of society, especially the consideration of relevant public policy formulation, fully reflects that it has long gone beyond the 'technology theory' and has assumed a comprehensive management perspective. Kurbalija (2016) has sorted Internet governance into eight areas: infrastructure, security, legal, economic, development, socio-cultural, and human rights. There are governance actors in every area. Internet governance is an umbrella structure, covering seven areas and more than 40 Internet public policy issues. A similar classification based on seven areas was used by the secretariat of the United Nations Commission on Science and Technology for Development in its April 2015 report 'Mapping of Public Policy Issues on the Internet' (UNCTAD, 2015). In line with this, the system of Internet governance which had at its core organizations that assumed responsibility for and ensured the allocation of basic resources and the determination of technical standards found that as the governance agenda became ever more complex, the shortcomings of a system and platforms built around technologies became ever clearer. As a result, more and more traditional organizations became engaged, while some new channels and platforms also emerged.

Looking back at this historical context, it can be seen that the development of Internet governance is accompanied by the popularization and penetration of technology, along with the promotion and maturity of national awareness. At present, the concept of cyberspace has become an important strategic space, governments, academia and other countries have formed a consensus, namely that [the concept of] the Internet does not cover all existing global digital development. The concepts of the information society and information and communication technologies are often considered to be more comprehensive, and the meaning of the two extends beyond the field of the Internet. Although different disciplines and fields have defined cyberspace from their own perspectives, there is a basic commonality: the Internet is considered to be only a part of cyberspace, and cyberspace should cover both Internet technology and network infrastructure, as well as human behaviour and relationships (historical social relations). President Barack Obama's cyber security policy assessment report in early 2009 referred to 'globally interconnected digital information and communications infrastructure' as cyberspace (White House, 2009, p. 1). The US Department of Defense and the US joint military doctrines define cyberspace as '[a] global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers' (e.g. DoD, 2019)

The Chinese 2016 National Cyberspace Security Strategy defines cyberspace as consisting of the Internet, communication networks, computer systems, automated control systems, digital devices and the applications, services and data it carries, and is 'a new channel for information dissemination', 'a new space for production and life', 'a new engine of economic

development', 'a new carrier of cultural prosperity', 'a new platform of social life', 'the new link of communication and cooperation' and 'the new frontier of national sovereignty' (CN, 2016).

Of course, cyberspace had its own uniqueness – both a virtual, man-made side, characterized by outstanding technical empowerment and a highly complex operation mechanism, and an integration with the traditional real world, with the boundary between the two becoming ever more blurred and even able to be ignored. This leads to a constant struggle between the application of existing theories, approaches, and mechanisms and the development of innovative theories, approaches, and mechanisms. But there is no denying that the trend of human dependence on digital technology will continue and even become more serious in the coming decades. These important technologies, including the Internet of Things, big data analytics, cloud computing, and artificial intelligence, will drive tremendous innovation and fundamentally change business, government, and society, and knowing how to maximize the opportunities and minimize risks posed by digital technology will be an eternal preoccupation.

Can international governance of cyberspace be equated with public policy issues related to the Internet or have a deeper and broader connotation? Can we continue to use the theory, framework and mechanism of Internet governance? Questions such as whether or not new mechanisms need to be created deserve serious consideration. The international governance of cyberspace includes infrastructure, standards, law, social culture, economy, development and so on, and its content needs to be more profound and wide-ranging than existing Internet governance, while the existence of structural contradictions is also more salient. The development of Internet governance embodies the law of technological development, initially concerned with the digital divide, universal access to services and the constant expansion and development of content, but once one takes into account the fact that Internet governance issues have not been fundamentally resolved, and technological developments have resulted in new challenges piling on top of and deepening existing problems, governance becomes more complex and difficult. In regard to the digital divide, the 2017 edition of the ITU annual measurement of the Information Society report states that while ICT is expanding rapidly, there is a significant digital divide between countries and regions. On average European states have the highest score in the 2017 ITU ICT Development Index (IDI) (7.50 points). Moreover, of the 40 countries in the region, 28 are in the top 25% of the rankings. The IDI average score for Africa (excluding the Arab countries of North Africa) is only 2.64 points (ITU, 2017). This problem will intensify as the data-driven innovation and production progresses. As Kai-fu Lee (2018, pp. ix–xi) predicts, AI 'relies on data to run, and this dependency continues to be consolidated across a wide range of industries: the more data you have, the better the product, the better the product, the more users you get, the more users you have, the more data you have', with the result that 'production capacity and wealth are concentrated in the hands of elite AI companies. Almost all of these companies are located in the United States and China'. The traditional digital divide and the digital divide in the era of AI cannot be talked of in the same way, and whether it can be solved will have a direct impact on the future development goals of the United Nations and even affect world stability.

Current status of international governance in cyberspace

International governance platforms

The process of important international governance platforms has been slow, primarily taking the form of ICANN reform. With the termination of the contract with the US Department of Commerce on 1 October 2016, the US government no longer exercises regulatory

authority over ICANN. But from the current process, the progress of reform is not obvious, and does not live up to expectations. Despite the US government's renunciation of ICANN's regulatory powers, the issue of jurisdiction remains of concern to the international community.

Making ICANN more reflective of its global objective, completely independent and free from the legal jurisdiction of the United States may require a long period of time. The international process has also slowed in terms of international rules and norms relating to security. Within the framework of the United Nations, the Group of Governmental Experts on Information security under the First Committee of the General Assembly (GGE) is in the process of developing a new round of negotiations. There is however significant disagreement within the international community on its working mode, membership representatives and outcomes and great power politics are much in evidence. On 8 November 2018, two resolutions adopted by the United Nations established two separate modalities for the future development of cyber security norms within the United Nations framework. The first was the Open-Ended Working Group, a Russian and Chinese initiative, convened in June 2019 and composed of all interested states, industry representatives, non-governmental organizations and academic institutions, to present its report to the General Assembly in the autumn of 2020 (UNGA, 2018a). The second, advocated by the United States, was the establishment of a new GGE, to further explore norms of conduct and how to implement confidence-building measures with a view to submitting a report to the General Assembly in the autumn of 2021 (UNGA, 2018b). In the area of international cooperation on cybercrime, the Commission on Crime Prevention and Criminal Justice under the United Nations Economic and Social Council (CCPCJ) established the United Nations Group of Governmental Experts on Cybercrime as the only platform for exploring international rules to counter cybercrime under the current United Nations framework. However, due to high levels of disagreement among the relevant parties regarding the ways in which the characteristics and harms of cybercrime have evolved, international responses and limitations and the development of comprehensive global documents, the expert group process has stagnated. Developed countries have a first-mover advantage in making the rules to combat cybercrime, and the use of the Budapest Convention to obstruct the development of global conventions and cooperation mechanisms makes it difficult for the international community to open a truly universal process of multilateral cooperation against cybercrime in the short term. The level of network development and external cooperation capacity of developing countries is inadequate and unbalanced, and overall coordination in promoting international rules against cybercrime has yet to be further enhanced. Relevant technologies and forms of cybercrime are still evolving, and the policy orientation and means of dealing with the problem of cybercrime in various countries are obviously different. The result has been that developing relevant international cooperation, in particular the development of a global convention against cybercrime, which will be a long and complex process.

The expansion of traditional international governance mechanisms

Some intergovernmental organizations that were not involved in Internet governance in the past, such as G20, G7, BRICS, ECDC, NATO, WTO, ILO and OSCE, are becoming key actors, and their participation in cyberspace governance is no longer reflected solely in the focus and setting of issues, but has taken the form of practical action. These traditional

institutions and platforms intersect with the technical organizations that have controlled Internet governance discussions over the past 20 years (especially ICANN, IETF, ISOC, RIRs, W3C, IEEE) to form a new 'governance complex'. Examples include: the launch of the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* by the NATO Cooperative Cyber Defence Centre for Excellence (Schmitt, 2017); the meeting of finance ministers of the G20 Group stressing that the malicious use of information and communication technologies endangers the stability of the financial system and focusing on the digital economy (DE, 2017); and the G7 statement of state responsibility in cyberspace which calls on the major technology platforms to join forces to resist propaganda by cyber extremists (G7, 2017). OSCE, for its part, wants to extend its confidence-building measures (CBM) globally (OSCE, 2016).

There is now a focus on the two major issues of network security and digital economy. In terms of cybersecurity issues, participation in discussions and governance have included the United Nations GGE, the Convention on Certain Conventional Weapons (CCW), the Security Council Counter-Terrorism Committee, ITU, the European Commission, the European Union, the African Union, Interpol/Europol, the Wassenaar Agreement, the Munich Security Conference, NATO, WSIS, IGF, OSCE, G7, BRICS, SCO, ASEAN, the Organization of American States, the Commonwealth, and the World Economic Forum (WEF), which were originally focused on traditional international security issues. Among them, the above-mentioned bodies focus on different areas and issues, such as GGE, OSCE, G7, BRICS, ECDC and WEF, which focus on norms of conduct of states and non-state actors in cyberspace; the Security Council Counter-Terrorism Committee, Interpol/Europol and WEF are also concerned with combating cyber terror. In addition, there are issues relating to the control of lethal autonomous weapons and dual-use technologies. At the United Nations Convention on Certain Conventional Weapons (CCW) conference, a group of governmental experts on lethal autonomous Weapons (LAWS) was established on December 16, 2016 with a mandate to study the emerging technologies of LAWS and assess their impact on international peace and security and to make recommendations for international governance. In October 2018, the Group of Experts submitted self-defeating reports after two meetings, in April and August, proposing ten guiding principles to regulate and guide state use of artificial intelligence for military purposes (UNOG, 2019). The United Nations has also divided issues relating to artificial intelligence into 14 areas, including cybersecurity, global governance, conditions for competition and international cooperation, in order to consider, in an integrated manner, the social, security, and ethical issues that may arise from the development of artificial intelligence.

Major cyber powers activism in governance

In the face of a severe security posture, the willingness of countries to seek international cooperation has increased significantly, but no strong leadership has yet emerged to dominate and promote international rule-making in cyberspace. From the breadth, depth and cutting-edge nature of cyberspace rule making, the United States undoubtedly retains an insurmountable advantages over other countries in the short term, and by virtue of this advantage, it translates domestic judicial measures, such as unilateral or bilateral, into international practice or global norms, such as the use of cyber-deterrence strategies and the unilateral use of prosecutions and sanctions to raise the costs for attackers. The new editions of the National Security Strategy (White House, 2017) and the National Cyber Strategy (White House, 2018) are explicitly intended to work with like-minded countries to build

and desired environment and related norms of responsible behaviour seeking to include as many stakeholders as possible in this cyberspace concept. To ensure, in particular the freedom of navigation and flow of information the US has become more explicit in shaping and governing the international commons through the provision of science, technology and leadership, the promotion of a particular reading of international law, and the protection of US interests in key institutions such as ICANN, IGF and ITU.

The EU, for its part, has become an important counterweight in the international governance of cyberspace through antitrust and data protection. To promote the realization of the ‘single digital market’, the EU aims to use the General Data Protection Regulations (GDPR) to create an international personal data protection paradigm, through a ‘digital tax’, ‘joint tax’ and other means to impose new controls on multinational Internet corporations, thereby enhancing the competitiveness of the European Union’s local digital industry and so regaining a central role in global cyberspace governance. Russia has been challenging the existing governance order in global cyberspace, and the new edition of the Information security doctrine, released at the end of 2016, clearly identifies the shortcomings of the current governance system and puts forward ideas for change, again trying to promote the construction of international cybersecurity standards, with proposals to build a backup global Domain Name System by 1 August 2018 to cover the BRICS countries. Russia has also submitted to the United Nations a draft United Nations Convention on Cooperation in Combating Information Crimes with a view to providing a global legal framework for combating cybercrime (RU, 2018), and has made its views clear on the role of the United Nations in cyberspace governance through the UN General Assembly resolutions. France is also champing at the bit and wants to make a difference. President Macron on the one hand wants to pursue a third way on Internet governance distinct from the proposals of China and the USA and to make a fresh start (Macron, 2018). On the other hand, the Paris Initiative for Cyberspace Information and Security was launched on the occasion of the 13th session of the IGF in November 2018, and nine norms of responsible State conduct were reaffirmed on the basis of the outcomes of international discussions such as GGE. China has also accelerated the pace of integration into the international governance system of cyberspace, speaking out through its own platform, the World Internet Congress, its participation in various comprehensive and multilateral mechanisms, with good results, and its ability to establish its agenda, its appeal and its influence are evident.

Non-state actors becoming active

These primarily take the form of global transnational corporations. Microsoft has promoted the Digital Geneva Convention initiative, and has persuaded more than 40 companies around the world to sign the Cyber Security Technology Agreement (CTA, 2019), describing the role of the state and private enterprises in ensuring cybersecurity, and proposing the creation of an international cyberattack traceability organization led by private enterprise to identify and trace cyberattacks undertaken or directed by states, and to provide technical evidence to governments, businesses and the general public. Microsoft has also further proposed the ‘Digital Peace initiative’ (Smith, 2017). In February 2018, Siemens assembled the Charter of Trust highlighting the responsibility and role of private companies in ensuring international cybersecurity (Siemens, 2019). On the basis of their technical advantages, these multinationals face national concerns about strategic technologies such as AI, and in response to the trust concerns of users around the world, are taking a lead in proposing their own governance solutions in areas such as AI. Microsoft has also promoted debate on the social role and

ethical consideration of artificial intelligence proposing to design a dependable AI, requiring a solution that embodies ethical principles and guiding it with social ethics while proving much greater computing power, and advocates six moral principles – ‘fairness, reliability and security, privacy and confidentiality, inclusion, transparency, responsibility’ – with the establishment of a commission to examine the development of artificial intelligence and the subsequent ethical standards of implementation (Smith & Shum, 2018). Google, for its part, advocates the AI seven principles, promising that four types of scenarios should not be applied to avoid AI causing or preventing increased social injustice, promising not to apply AI to weapons development, not to violate human rights norms for monitoring and gathering information (Pichai, 2018).

A number of emerging non-governmental platforms are also rising rapidly. For example, the Global Commission on the Stability of Cyberspace (GCSC) has since its inception in 2017 proposed ‘six new global norms for both state and non-state actors to help promote the peaceful use of cyberspace’. They *inter alia* include norms to avoid tampering, against commandeering of ICT devices into botnets, reduce and mitigate ‘significant vulnerabilities’, and against offensive cyber operations by *non-state actors* [emphasis added] (GCSC, 2019).

New themes of governance

New topics are gradually becoming integrated into the scope of international cyber governance. All major negotiations on international economic and trade rules have now incorporated Internet-related issues. Through negotiations on digital commerce, telecommunications, investment and intellectual property rights in the Trans-Pacific Partnership Agreement (TPP) has formed a systematic international economic and trade rule proposition related to the Internet, known as the ‘digital article 24’, which has far-reaching implications for the formulation of relevant international rules. The United States, the European Union and China, Brazil, Mexico and others have submitted more than 30 proposals to the WTO in an attempt to delineate the agenda for the forthcoming multilateral negotiations on trade rules for electronic commerce, suggesting topics such as allowing data to flow across borders, opening up networks, limiting the localization of computing facilities, protecting critical source codes, prohibiting forced technology transfer, the prohibition of mandatory use of local technologies, the maintenance of market-oriented standardization and global interoperability, the promotion of multi-stakeholder participation in regulations and standard-setting, the protection of personal information, the fight against cybercrime. At present, the relevant negotiations are focused on digital trade barriers, including data localization requirements, tariff barriers, intellectual property protection measures and cultural barriers

From this, it is clear that countries have very different concerns, and even the understanding and definition of some issues are not the same. Under the framework of WTO, rules originally based on trade in goods are not well-suited to the needs of the digital economy and digital trade, and some original regulations or consensuses are being challenged by new problems. On 12 April 2018, the United States submitted to the WTO a proposal for a Joint Statement on E-commerce Initiatives, proposing that seven issues, namely, the free flow of information, fair treatment of digital products, proprietary information protection, digital security, the promotion of Internet services, the creation of a competitive telecommunications market and digital trade should be treated in line with WTO Preferential Measures which include the free flow of information and the copying of existing rules to include cross-border transfer of data, prevention of data localization and prohibition of network shielding (US, 2018). In relation to proprietary information protection the United States

advocated the development of rules in the areas of protection of source codes, prohibition of forced transfer of technology and prohibition of discriminatory technical requirements. Digital security requires the legislation of digital encryption technology, and the United States also replaced the term 'E-commerce' in the statement with 'digital trade', with the clear intention of controlling the narrative and laying the foundation for a digital trading system under the framework of the future WTO (US, 2018).

In addition, new threats from the uncertainty of the development of new technologies such as artificial intelligence, the Internet of Things, and blockchain are beginning to attract the attention of governance circles, with new concerns beginning to emerge, such as autonomous vehicle safety issues, the regulation of cryptocurrencies, algorithmic biases, and the 'deep fake' problem enabled by artificial intelligence are all the subject of intense investigation with relevant concepts, mechanisms, platforms, action plans constantly being put forward. But it is unfortunately the case that methods for avoiding a disconnect between technology, industry and policy, and focusing on some security issues while ignoring others have not received sufficient attention.

Characteristics of international governance in cyberspace

In general, conflict and cooperation co-exist in the international governance of cyberspace, exploration and practice are being constantly developed, some basic principles and rules have reached consensus and been put into practice. But the inherent contradictions in governance mechanisms, the difficulties of the balance of interests of all parties and so on are still hindering process towards a multilateral, democratic and transparent direction.

The diversity of governance issues and agendas and the complexity of mechanisms

At the main level, governments, international organizations, technical communities, enterprises, individual experts, and research institutions are involved in the operation of the Internet technology architecture. In their distinct roles and capacities, they are responsible for the development of specific standards and agreements to provide policy and technical guidance for Internet operations. As a consequence, common understandings are proving elusive, consensus is hard to reach and there are few governance models and rules that are widely recognized and in fact have significant utility in responding to threats and risks in cyberspace. At the topic level, cyberspace involves a wide range of areas, with deep embedding of political, economic, social, cultural and military factors. The Internet is no longer seen as a sectoral issue and is beginning to play a pivotal role in discussions on global political issues such as international security, economic development, trade, the environment and human rights, resulting in almost all traditional public policy issues involving the Internet. At the mechanism level, there is not only the question of complexity in relation to the operating and policy processes in regard to the governance of a particular area or issue but also the problem of how to interact, communicate and operate among many different governance issues.

As countries, non-governmental organizations, the private sector, businesses, and even individuals can participate in the governance process, the status of each actor, the role played, and the power game between them, are more complex in this 'cooperative, decentralized ecosystem of governance'. Moreover, the distribution of resources and capacities among the parties is extremely uneven, unlike traditional international mechanisms. The control that

governments and international organizations can exert is weaker than that of traditional international mechanisms. However, as public policy has achieved greater salience, national governments have begun to wake up to pay greater attention to participating in governance. At the same time, while the projection of national power is increasing the comprehensiveness and effectiveness of governance, possible solutions to problems have become more varying and complex. The game played between the states that lie behind international Internet governance, in particular the major powers, has become more densely textured. It can be ascertained that no one institution or organization has control over the collective decision-making of all Internet issues, that different institutions or organizations deal with diverse issues and that decision-making methods and procedures are not the same, and that because of the speed of network development, short-term approaches tend to dominate, and the issues that the same organization focuses on at different times vary. Similar approaches to decision-making and procedures cannot be reused, and a unitary decision-making process in different areas of governance will not be universally applicable.

The coexistence of competition and cooperation, consensus and disagreement

The multi-actor-multi-layer *problematique* is epitomized by the interaction between states, states and the private sector around issues such as freedom and regulation, development and security. At the inter-state level, international cyberspace governance is increasingly influenced by *Realpolitik*; the governance agenda has become a tool of a strategic game for the major global powers, the protectionist sentiment represented by some major Western countries is obviously heating up, the phenomenon of ‘reverse globalization’ is rampant, and problems of network security and data protection are constantly politicized and made into economic issues. There are frequent cases of digital protectionism around the world. For example, the United States has barred Kaspersky products, Australia has banned Huawei from participating in its 5G construction, and both the United States and the European Union are stepping up security reviews for investment in high-tech areas, greatly increasing distrust between states (e.g. Keane, 2019). However, cyberspace governance is, after all, a global issue, especially the digital economy and development issues are the common interests of all countries, but require ever greater co-operation. Network characteristics determine that only cooperation can deliver security and stability and that joint exploration of areas of cooperation between countries engaged in competition and confrontation will be the norm for future governance

At the level of government and private sector, there is a contradiction between public interest and enterprise interests. On the one hand, the prevailing phenomenon of super-platform monopolies is subverting traditional forms of governance. Within a country, online platforms are replacing important government functions in providing public services and shaping public policies; internationally, sovereign states that have played a leading role in global governance have sometimes had to succumb to super-network platforms. Enterprises, due to business models based on the collection, storage, analysis and sale of data, and the need of enterprises to promote the free flow of global data to develop demand for the digital economy, are in conflict with the government’s need to guarantee social order and civil rights and even national security. With the deepening of the international rules of conduct in cyberspace the current focus is on how to implement the norms that have been agreed, and objectively there is the question of how to include the private sector in this process, whether through rules or treaty formulation which originally was the sole prerogative of

governments, should be extended to non-state actors such as private-sector enterprises. On the other hand, the role of major platforms in providing public services and social media leads to the discussion of how to constrain the private sector or determine its level of social responsibility. ‘Cyber electoral interference’ (the case of Cambridge Analytica), cyber terror, cyber bullying, online hate speech and other phenomena are all widespread. In terms of content control, governments and the private sector have taken joint action against false news and extremist and terrorist content. At the corporate level, companies such as Facebook, Twitter, Google and Wikipedia have invested a lot of manpower, technology and money in content management. At the government level, the main measures taken are heavy penalties (Germany, Australia), the allocation of special governance funds (United States), the establishment of specialized regulatory bodies (Singapore), tax regulation (UK), the issuance of governance guidelines (EU).

The internal contradictions of international cyber-governance mechanisms becoming prominent

Since 2005, the international community has begun to discuss the connotations and mechanism of Internet governance from the perspective of comprehensive management, and a framework mechanism for multi-stakeholder joint governance has been determined. However, with the rapid development and full integration of ICT, the inherent ‘inadequacy’ of this mechanism is constantly exposed. This manifests itself in two ways: first, the contradiction between the integration and fragmentation of governance mechanisms. Admittedly, as Internet governance moves towards international governance of cyberspace, it cannot be denied that governance areas and issues have become more diverse and complex, covering all issues related to the development and use of the Internet in addition to maintaining the technical framework, but also involving Internet use-related issues (including spam, cybersecurity and cybercrime), Influencing areas that transcend the Internet itself (such as online intellectual property rights, international trade issues arising from the network economy) and other Internet development issues (such as the digital divide and network capacity-building in developing countries). It is not possible for a rule to apply all situations, and rule-making must be divided into areas, sub-topics and forms of flexibility involving a mixture of written and unwritten rules. At the same time, this specialization can easily produce an ‘echo chamber’ effect or ‘group polarization’, objectively resulting in the decentralization and fragmentation of governance, and even the emergence of contradictory outcomes in decision-making.

In addition, the lack of overall coordination between different platforms and mechanisms is becoming increasingly prominent. There are two dimensions to the coordination of cyberspace governance mechanisms, namely, horizontally between international governance institutions, and vertically between ‘multiple subjects’. On the one hand, the establishment of Internet governance institutions with comprehensive management ability has basically taken shape, but there is a lack of coordination mechanisms among agencies, which cannot promote the integration of resources well, so it cannot form an effective joint force. Duplication and overlapping functions are common in the governance process, and the relevant policies lack universal applicability and authority. The main reason for this phenomenon is that the functional definition of Internet governance institutions does not set strict boundaries. The limits of governance areas and issues depend on the statutory documentation constraints at the time of the establishment of the institution, reflecting the interests of member states, but in many cases the statutory documents set up by the institution do not set clear

boundaries for the establishment of the organization's issues. On the other hand, the security maintenance of cyberspace must be carried out by various entities, including government, the private sector, non-governmental organizations and the vast number of network users. However, it is obvious that the mechanism of state sovereignty as the basis of power, 'top-down' and 'integrated management' of the government cannot be replicated in cyberspace. To date, the international community has not found an effective mechanism to provide an effective platform for the formation of synergies among the various issues.

Second is the conflict between fairness and efficiency under the multi-stakeholder model. In cyberspace governance, governance at the technical level is dominated by the private sector, and the social public policy dimension is jointly dominated on an equal footing by a wide range of actors, including governments, the private sector and non-governmental organizations, while the economic and security dimensions are nationally led multilateral models. The first type of governance participation is the first-tier institutions represented by ICANN, IETF and ITU, which form the basis of current Internet governance mechanisms and focus on the technology architecture and development of the Internet. The institutions responsible for international standard setting, such as IEEE, IEC and ISO, are also part of this. The second layer of participation in cyber governance comprises the WGIG and IGF under the framework of the United Nations, which specializes in integrated Internet governance institutions, while the latter is an open forum on Internet governance. The third type of participation in governance takes the form of governments and intergovernmental organizations. Overall, Internet governance has identified a multi-stakeholder model from the outset, reflecting the openness, freedom and innovation of the Internet as a new technology through bottom-up, open and public processes and equality between all parties. Governance decision-making is an exercise in 'public policy', which requires all parties to jointly formulate and implement principles, guidelines, rules and programmes, but because of different national conditions, the fact that the subject is complex and borderless, there are too many participants, multiple platforms, especially by the non-governmental actors acting as prima donnas and turning their platforms into talking shops the result is much talk but few decisions. For example, the IGF is more of a platform for discussion and cannot formulate cyberspace consistent norms while institutions led by private companies, civil society and the technology community have agreed on technical code, corporate self-discipline, or a legally unenforceable commitment, but these voluntary decisions cannot be reflected in national policies and do not achieve actual governance results. While the traditional bottom-up approach to Internet governance is conducive to ensuring equality and openness, it also results in relatively low efficiency with the introduction of a policy requiring a comprehensive worldwide range of views, universal support and basic unanimity. Therefore, the negation of a resolution is much more efficient than the adoption of a resolution. In addition, the rapid development of technology and the long consultation process required for rule-making, delays in national legal approval, passive responses and so on are also very mismatched.

Exploring solutions for resolving Internet governance dilemmas

The shift from Internet governance towards concepts, mechanisms and models for international cyberspace governance is at a critical period of re-appraisal. Given the characteristics of current international cyberspace governance summarized above, structural reform and innovation at the mechanism level should focus on solving the contradictions and conflicts between existing mechanisms, such as the integration of governance issues and the fragmentation of mechanisms, the contradictions and clashes between fairness and efficiency

in the multi-stakeholder model, and the formation of a diversity of the Internet, sustain the diversity of platforms, actors and the multiparty participations that characterizes the existing Internet but also act as a channel (mechanism or platform) that can comprehensively assess the demands of all parties, integrate the platform governance programme, comprehensively weigh up the inclusion of issues and progress, while maintaining flexibility and adaptability as a way to better deal with the uncertainty brought about by technological development.

As Kurbalija (2016) has put it, stakeholders should identify priority issues based on their particular interests: thus, while choosing a branch of the tree, they should not ignore not ignore the forest of Internet governance issues. Kleinwächter (2018), too, has pointedly highlighted this dilemma. He believes that 20 years ago, Internet governance was a technical issue that had political implications. Today, Internet governance has become an important political issue that contains a number of technical elements. This time shift is challenging the balance of mechanisms within the global Internet governance ecosystem, as well as intergovernmental and non-governmental negotiating mechanisms. The involvement of a variety of actors requires the emergence of an 'Internet governance complexity' the inclusion of Internet experts in public policy circles, and greater government attention to discussions of technical issues. This has led to parallel and partial competitive negotiating structures and cultural conflicts, resulting in a very diverse and fragmented process of consultation and discussion of network-related matters, with different groups and stakeholders confined to their own areas and often ignoring what is happening in other areas. In January 2018, after four years of wrangling, the UNCSTD 'Working Group on Strengthening Cooperation' has not reached a consensus on how to strengthen cooperation on Internet governance in the future. Kleinwächter argues that 'cyberspace is too big to be managed by a single community or group of stakeholders' (Kleinwächter, 2015), but is now at a 'crossroads' where different management concepts/approaches need to find a way to coexist, learn from each other and collaborate to save cyberspace. A new wave of wisdom is needed to bring about this new complex and the impending transfer of power from the Internet governance ecology towards a new balance. And this rebalancing of forces will drive an innovative governance path

Admittedly, the reality is that cyberspace does not have a single organization with sufficient authority to implement all norms 'from top to bottom', but consists of an organizational collective comprising a series of loosely related organizations concerned with specific topics and norms, all ploughing their own furrows but also linked by many connections which are collectively exercising a governance function. So, is there a need for such a single institution, or should the focus be on improving the status quo to overcome current governance problems? A platform such as the IGF which allows multi-stakeholder discussions across sectors and groups has limitations and lacks a more comprehensive, holistic approach. Kleinwächter (2015) notes that, on the one hand, there is an objective need for an all-encompassing channel linking various intergovernmental, non-governmental platforms for negotiation and discussion. On the other hand, this risks of creating an 'illusion' that all these network-related public policy and technical issues can be integrated into a single consultative process, as has been the case with the United Nations Convention on the Law of the Sea and the Framework Convention on Climate Change. A more realistic approach would be to establish a broad, central and flexible framework that promotes and enhances communication and collaboration among the various levels and promotes formal or informal cooperation between different platforms and channels. All platforms and groups can be linked through focal points and mutual reporting mechanisms. In Kleinwächter's (2018) view, global intergovernmental negotiations on disarmament, the environment, trade or development issues were not inter-linked. But with the Internet, all issues are connected. A new technology agreement can have

a significant impact on cybersecurity, business models, and the strengthening or weakening of human rights. The same is true of political decision-making. He argues that the framework of the new mechanism could either emanate from existing mechanisms such as IGF, WSIS or NetMundial, or that it could be a completely new, independent initiative. One approach could, similarly as the OCSE ‘Helsinki process’ in the field of regional security cooperation, include ‘basketing’ governance issues and agendas. To that end, he proposes four options: the IGF model; the WSIS+20 model; NetMundial+5; and a completely new independent process

The United Nations has also been concerned with this issue and has been striving to introduce innovation. In 2018, Secretary-General Gutierrez created a high-level digital co-operation group (High-Level Panel on Digital Cooperation) to reconcile the imbalances and inconsistencies in the international governance mechanisms of cyberspace. The mandate of the group is to consider from the perspective of the socially and economically disruptive impact of digital technology how to build a secure and inclusive digital future for all, taking into account relevant human rights norms (UN, 2018). To this end, Mr. Gutierrez has assembled representative figures in the field to engage in comprehensive consideration of digital co-operation, confidence-building measures, data security and other issues through consultation, research and reporting with a view to producing a report by May 2019. Kleinwächter has welcomed this move, making the point that the panel is rooted in the digital world of the future and arguing that the complexity of Internet governance has given rise to a new need to move beyond the government-led and non-governmental, multilateral or multi-party divisions of the past fifteen years and to reflect on the shared responsibility of all in the digital world of the future. But he is also concerned about how the panel’s report translates into concrete action, as otherwise it risks becoming ‘sooner or later submerged in the vast stack of documents of the United Nations’ (Kleinwächter, 2019). Notably, Secretary-General Gutierrez has consistently emphasized the United Nations as a promoter (facilitator) rather than a manager or controller when promoting the panel.

At its root, there are still two fundamental issues that need to be clarified. One is how to clearly define the concept of governance, including what is international cyberspace governance, what should be governed, how it should be governed, what is the status and role of government and whether new mechanisms/treaties/conventions are needed and, in the final analysis, there is a values-driven contest to determine the kind of concepts of cyberspace and cyberspace governance will emerge. With the expansion of the connotation and extension of governance, there is a tendency to include all network-related affairs, and with the deep integration of real space and cyberspace, some traditional mechanisms and systems are also gradually considering network-related problems including how to deal with the relationship between the old and the new mechanisms. For example, there remains a dispute about what are the most appropriate mechanisms for resolving pressing discussions on rules for digital trade. The other question is that of how governance reform can respect the unique character and future development trends of the Internet (or cyberspace), taking into account the existence and demands of state and non-state stakeholders, fair processes, transparency, and inclusivity.

References

- China (CN) (2016) *National Cyberspace Security Strategy*. Available from: <https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/> [accessed 2 August 2019].
- Cybersecurity Tech Accord (CTA) (2019) *Tech Accord*. Available from: <https://cybertechaccord.org/> [accessed 2 August 2019].
- [US] Department of Defense (DoD) (2018) *Summary. Department of Defense Cyber Strategy* (September).

- [US] Department of Defense (DoD) (2019) DOD Dictionary of Military and Associated Terms. Available from: www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf [accessed 2 August 2019].
- [German] Federal Ministry of Finance (DE) (2017) Meeting of G20 finance ministers and central bank governors in Baden-Baden, Germany. Available from: www.bundesfinanzministerium.de/Content/EN/Standardartikel/Press_Room/Publications/Technical-Papers/2017-04-27-meeting-g20-finance-ministers.html. [accessed 2 August 2019].
- Global Commission on the Stability of Cyberspace (GCSC) (2018) *Norm Package Singapore*. Available from: <https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf> [accessed 2 August 2019].
- Group of Seven (G7) (2017) G7 Taormina Statement on the Fight Against Terrorism and Violent Extremism. Available at: www.g7.utoronto.ca/summit/2017taormina/statement-on-terrorism-and-extremism.html. [accessed 2 August 2019].
- International Telecommunication Union (ITU) (2017) ICT Development Index 2017. Available from: www.itu.int/net4/ITU-D/idi/2017/index.html [accessed 2 August 2019].
- Kai-fu Lee (2018) *AI Superpowers: China, Silicon Valley, and the New World Order*. New York, Houghton Mifflin Harcourt Publishing.
- Keane, S. (2019) Huawei ban: Full timeline on how and why its phones are under fire. Blog. Available from: www.cnet.com/news/huawei-ban-full-timeline-on-how-and-why-its-phones-are-under-fire/ [accessed 2 August 2019].
- Kleinwächter, W. (2015) IGF, WSIS 10+ & WIC: Three world conferences for one Internet. Blog. Available from: www.circleid.com/posts/20151221_igf_wsis_10_wic_three_world_conferences_for_one_internet/ [accessed 2 August 2019].
- Kleinwächter, W. (2018) Towards a holistic approach for Internet related public policy making. Can the Helsinki process of the 1970s be a source of inspiration to enhance stability in cyberspace? *GCSC Thought Piece* (January). Available from: https://cyberstability.org/wp-content/uploads/2018/02/GCSC_Kleinwachter-Thought-Piece-2018-1.pdf [accessed 2 August 2019].
- Kleinwächter, W. (2019) Instability in Cyberspace is as Dangerous as Climate Change: Towards a New Deal for Digital Cooperation. Paper prepared for the UN High Level Panel on Digital Cooperation. Available from: https://digitalcooperation.org/wp-content/uploads/2019/02/Wolfman_Kleinw%C3%A4chter_CFC-Individual-Submission-1.pdf [accessed 2 August 2019].
- Kurbalija, J. (2016) *An Introduction to Internet Governance*. Geneva, DiploFoundation.
- Macron, M.E. (2018) Speech at the Internet Governance Forum (12 November). Available from: www.elysee.fr/en/emmanuel-macron/2018/11/12/speech-by-m-emmanuel-macron-president-of-the-republic-at-the-internet-governance-forum [accessed 2 August 2019].
- Mueller, M. (2010/2017) Internet Governance. In *Oxford Research Encyclopedia*. Available from: DOI: 10.1093/acrefore/9780190846626.013.245 [accessed 2 August 2019].
- Organization for Security and Co-operation in Europe (OSCE) (2016) OSCE Confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. PC.DEC/1202 (10 March).
- Palfrey, J. (2010) Four phases of internet regulation. *Social Research*. 77(3): 981–996.
- Pichai, S. (2018) AI at Google: Our principles. Blog. Available from: www.blog.google/technology/ai/ai-principles/ [accessed 2 August 2019].
- [The] Russian Federation (RU) (2018) Draft United Nations Convention on Cooperation in Combating Information Crimes. Available from: www.rusemb.org.uk/fnapr/6393 [accessed 2 August 2019].
- Schmitt, M.N. (ed.) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press.
- Siemens (2019) The Charter of Trust takes a major step forward to advance cybersecurity. Available from: <https://press.siemens.com/global/en/feature/charter-trust-takes-major-step-forward-advance-cybersecurity> [accessed 2 August 2019].
- Smith, B. (2017) The need for a digital Geneva Convention. Blog. Available from: <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/> [accessed 2 August 2019].
- Smith, B. and Shum, H. (2018) The future computed: Artificial intelligence and its role in society. Blog. Available from: <https://blogs.microsoft.com/blog/2018/01/17/future-computed-artificial-intelligence-role-society/> [accessed 2 August 2019].

- United Nations (UN) (2018) Secretary-General's High-level Panel on Digital Cooperation. Available from: www.un.org/en/digital-cooperation-panel/ [accessed 2 August 2019].
- United Nations General Assembly (UNGA) (2018a) Developments in the field of information and telecommunications in the context of international security. A/C.1/73/L.71. (8 November).
- United Nations General Assembly (UNGA) (2018b) Advancing responsible State behaviour in cyberspace in the context of international security. A/C.1/73/L.72 (8 November).
- United Nations Commission on Science and Technology for Development (2015) Mapping of international Internet public policy issues. Report E/CN.16/2015/CRP.2. Available from: https://unctad.org/meetings/en/SessionalDocuments/ecn162015crp2_en.pdf [accessed 2 August 2019].
- United Nations Office at Geneva (UNOG) (2019) Background on Lethal Autonomous Weapons Systems in the CCW. Available from: [www.unog.ch/80256EE600585943/\(httpPages\)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument](http://www.unog.ch/80256EE600585943/(httpPages)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument) [accessed 2 August 2019].
- United Nations (2005) Report of the Working Group on Internet Governance. Available from: www.wgig.org/docs/WGIGREPORT.pdf [accessed 2 August 2019].
- [The] United States (US) (2018) U.S. Statement at the Meeting of the WTO Joint Statement Initiative on E-Commerce. Available from: <https://geneva.usmission.gov/2019/03/06/u-s-statement-at-the-meeting-of-the-wto-joint-statement-initiative-on-e-commerce/> [accessed 2 August 2019].
- [The] White House (2009) *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*.
- [The] White House (2017) *National Security Strategy* (December).
- [The] White House (2018) *National Cyber Strategy* (September).
- World Summit on the Information Society (2003) *Geneva Action Plan*. Available from: www.itu.int/net/wsis/docs/geneva/official/poa.html [accessed 2 August 2019].

THE BECOMING OF CYBER-MILITARY CAPABILITIES

Mirva Salminen and Mika Kerttunen

Introduction

Although an early manifesto did not welcome governments into cyberspace (Barlow, 1996), it is questionable whether cyberspace has ever been truly civilian. The newcomers have not been governments with their claims of sovereignty and methods of enforcement, but civil societies. Already in the 1940s, computing power was utilized to calculate flight paths and trajectories, as well as to break the atom; the United States and the Soviet Union connected early warning sensors to computerized command and control stations and to fire and manoeuvre units in the 1950s; advancements of the US Department of Defense Advanced Research Projects Agency (ARPA) experimental network paved way to civilian research and commercial utilization of increased connectivity. Digitalization in the 1980s and 1990s made a qualitative shift by improving the performance of all military functions – a tendency that signifies the anticipated utility of contemporary information and communications technologies (ICTs) and emerging technologies such as machine learning, artificial intelligence, and quantum computing.

In this chapter, we are interested in the assumed militarization of cyberspace and its possible impact on international peace and security. It has been claimed that digitalization of the battlefield is ‘gamifying’ war (Der Derian, 1992), thus detaching soldiers’ experience from the realities of warfare, or threatening international peace and security, even human life, like the weapons of mass destruction (RU MFA, 1998). Reports and reporters of digital and cyber arms race add weight to this doctrine of digital militarization (e.g. CSIS, 1998). An additional strand in the debate, traceable via Paul Virilio (e.g. 2005/1998) and Michel Foucault (1995/1977) all the way to Jeremy Bentham (Božovič, 1995), emphasizes how the state apparatus utilizes advanced military and law enforcement technologies to monitor, control and/or suppress political opinion and the individual.

Our analysis begins with the diffusion of innovations and militarization. Departing from this conceptual foundation, we investigate how and why countries are developing cyber military capabilities. Here, we explore two examples of well-documented approaches, namely the United States and the Netherlands. We do not intend to shame or blame these countries – on the contrary, the respective governments can be congratulated for clarity and transparency that the majority of countries dealing with, or claiming to deal with, similar

issues seriously lack. The US and Dutch stories, we are confident, have significance beyond these countries as they witness some of the most profound processes of militarization in the field of information and cybersecurity.

We finalize our analysis by discussing whether the proliferation of cyber military capabilities, a.k.a. militarization, can be considered problematic, even threatening, to international peace and security, as well as to domestic, regional and global stability. When investigating military proliferation of (any) technology, the purest of horizontal (quantity) and vertical (quality) proliferation are not sufficient meters – or calls for alarm. We will add to the debate a political layer which pays close attention not only to the politics of proliferation but also to the conducted (or claimed) policies. Thus, the proliferation of ICTs neither makes any state nor prohibits any state from becoming militant. Moreover, it does not prevent a state from potentially or factually threatening international peace and security. Indeed, we may tentatively ask whether some cyber-savvy governments are actually considering their day to have come.

The diffusion of innovations, securitization, and becoming militant

The joining together of computer, information, and network security, of critical infrastructure protection, and safeguarding of the functions vital to society or national security can be understood as innovative – an innovation labelled cybersecurity. While the concept of innovation is both elusive and ubiquitous, it can be given some clarity by defining it as an outcome, a process, and a particular kind of mindset. As an outcome, innovation refers to, for instance: new products, services or programmes; changes in methods or processes; novel ways of interacting with stakeholders; or organizational changes. Innovation as a process, again, means the ways of organizing innovation so that the desired outcomes come to fruition. Finally, as a mindset, innovation addresses both individuals' adoption of it and organizational cultures that support it (Kahn, 2018). Even if the majority of research literature discusses innovation in the private sector, it can and also has been considered as a novel idea initiated by a public sector organization along the aforementioned aspects (Demirciogly & Audretsch, 2017). All aspects of innovation are present in the ongoing (national) organization of cybersecurity, which also entails its militarization. Whether the use of the prefix 'cyber' in the security context originated from the private or public sector is of secondary importance. The main point is that states around the world have adopted the concept for national security purposes.

Once having emerged, innovations do not sit with the organization that has generated them but tend to diffuse. According to Rogers (2003, p. 5), '[d]iffusion is the process in which an innovation is communicated through certain channels over time among the members of a social system'. Communication about innovations is 'a [two-way] process in which participants create and share information with one another in order to reach a mutual understanding' (pp. 5–6). However, getting the idea adopted by the social system is difficult and time-consuming (p. 1). With regard to cybersecurity, this difficulty manifests itself, for instance: in organizations' observed slowness in composing and executing cybersecurity plans, strategies, and programmes; training personnel; and integrating cybersecurity in core business functions and continuity management (Lehto et al., 2017; 2018; see also Tikk, 2017, p. 159). Next to that, the difficulty can be read into the continuous concern over the individual being the 'weakest link in cybersecurity' due to his or her gullibility or malevolence (e.g. Salminen, 2019, p. 325).

Regardless of the difficulty experienced in the dissemination of cybersecurity practices within societies, the spread of ICTs and their use is worldwide. Digitalization is changing

societies, which transforms the ways of warfighting. Thus, it is not only military use of technology that affects the way cybersecurity is conceptualized, but also, and more importantly, the developments taking place in wider society have an impact upon military organization and its way of operating (Keegan, 2005; Demchak, 2011; Junio, 2012). Ever furthering the digitalization of societies feeds into a general concern over the continuity of their functions and vulnerability, which generates room for advocating military responses in the name of national security. As the effective use of ICTs generates an advantage in warfighting, there have been attempts to obstruct the diffusion of such technologies – which in effect militarized ICTs from the very beginning. When it became clear that the spread of these technologies could not be prevented, the US administration's response was to lower barriers of entry and free exports – excluding the very heart of military technologies such as encryption codes (Arquilla, 2003, p. 358; Singer & Friedman, 2014, pp. 16–21; about the commercialization of Internet, see e.g. Greenstein, 2015). Currently, the diffusion of those very pivotal technologies still takes place via commercial and/or politically motivated espionage (e.g. Healey & Grindal, 2013, p. 69).

To quote Myriam Dunn Cavelty (from Chapter 1), with reference to Barry Buzan et al. (1998), '[s]ecuritization signifies the representation of a fact, a person, or a development as a danger for the military, political, economic, ecological, and/or social security of a political collective and the acceptance of this representation by the respective political addressee'. Invoking security thus helps legitimize the use of extraordinary means for response, as well as remove the matter from ordinary political processes (Wæver, 1995). According to Ronald J. Deibert (2017, p. 172), the securitization of cyberspace may be the most important factor that is currently changing communications worldwide. Militarization, then, refers to an extreme strand of securitization that claims the priority of military means in responding to the securitized state of affairs (Wæver, 1995; with regard to cyberspace, see, for example, Healey & Grindal 2013, p. 64, 164). It operates in both ideational and material realms by framing an issue as a military matter (about the framing of cybersecurity see, for example, Dunn Cavelty, 2008; Finnemore & Hollis, 2016). This takes place, for instance, by constructing and maintaining a discourse that utilizes familiar military expressions and discursive formations that distinguish the matter from other possible responses within securitization (e.g. Kan, 2013, pp. 111–112; Gomez & Villar, 2018; about discursive formations, see Foucault, 2009). Thus, claiming resources for a military response, establishing relevant organizations and positions to deal with the matter, and operationalizing newly composed or renewed strategies, concepts and programmes for carrying out the task becomes possible (with regard to cyberspace, see e.g. Barnard-Wills & Ashenden, 2012; Healey & Grindal, 2013, pp. 64–67, 73–78). Discursive and material practices that constitute cybersecurity and frame it as a military matter are tightly intertwined (about discursive and material practices, see Foucault (2009); also e.g. Alhanen (2007)). Together they increase the pressure on and the willingness of states and their armed forces 'to develop the capacity to fight and win wars in [the cyber] domain' (BAS, 2011, p. 2).

By implication, the 'proof' of successful securitization is institutional reactions (of all sorts) and the persuasion of unnamed audience. This is a low benchmark for something to be securitized. In fact, if any kind of policy reports or institutional responses are a proof of successful securitization, it starts to encompass everything that takes place in policy processes. While this might be a deliberate choice depending on what one wants securitization theory to be, it comes with a certain 'cost', such as losing the initial focus of the theory. According to Eneken Tikk (2017, p. 151), regardless of the framing of cybersecurity in terms of urgent military threats and weaponization of information, there is

insufficient evidential ground and support [for the framing] in actual international affairs. While states have generally come to regard cyber security and cyber defence as matters of national strategy, policy and legislation, little in their activities speaks of true threat of cyber arms race, let alone increased likelihood of ICT-driven international conflict.

Thus, the securitizing and militarizing acts in cybersecurity seem to reflect more the potentialities and fears embedded in digitalization than the current state of affairs. Nonetheless, they construct societies and their mutual relations, for which reason framings and (un)succesful securitization/militarization attempts matter.

Multiple examples of attempted militarization of cybersecurity are available in International Relations and Security Studies literature as the approach emerged in the 1990s (e.g. Arquilla & Ronfeldt, 1993) and properly took off in the twenty-firstst century (e.g. Libicki, 2009; Kramer et al., 2009; Clarke & Knake, 2010; Demchak, 2011; Carr, 2012; Healey & Grindal, 2013; Rantapelkonen & Salminen, 2013). At the time of writing, Amazon US's book webstore provides 370 hits for 'cyberwar' and 966 hits for 'cyber war' without taking into account other possible war-related word combinations with the prefix 'cyber'. Cyberwar discourse builds on earlier strands of theorizing on, as well as practices of, for example, electronic warfare, information warfare and network centric warfare (e.g. Demchak, 2003; Junio, 2012). Highlighting of intelligence capabilities after 9/11 paved the way for accelerating militarization of cybersecurity, when states began to understand cyberspace not only as a source of intelligence, but also as a battlefield (Deibert, 2003; BAS, 2011). The fifth domain of cyberspace was included in the fighting environment model, which already comprised the domains of land, sea, the air, and space.

The techniques used for militarization include strategization of the matter; that is, conceptualizing and understanding cybersecurity within the military vocabulary and logic (for an example of such an activity, see Kramer, 2009). This can be seen as the qualitative dimension of militarization. Information and communication technology focused the information security field and already utilized the language of attacking and defending long before states became interested in cyberspace as a field of military operations (for an example of the language of information security, see e.g. Workman et al., 2013). Yet, with increased state interest the matter has been lifted from the level of individuals and corporations to the level of societies, states, and inter-/transnational organizations. According to the logic, society is under threat and the military ought to defend it – in cyberspace as elsewhere. Strategization entails, for instance, identifying the threat(s) and the enemy/ies. Commonly utilized threat typology in national cybersecurity strategies includes hacktivism, cybercrime, digital espionage, cyber terrorism, and cyber operations. The military is to worry about the last three of these threat categories (e.g. Healey & Grindal 2013; Limnéll et al., 2015). The corresponding enemy imagery then consists of digital spies, cyber terrorists, and cyber warriors – all of whom can operate on behalf of rivalry states, individuals or groups with political or economic motivations, as well as for corporations or opportunistic groups with or without a connection to rivalry states. The difficulty of the technical attribution of cyber-attacks is acknowledged in the discourse, but this does not prevent strategic or political attribution being used for the legitimization of selected countermeasures, requests for additional resources, and/or reorganization of (national) security production (about the different forms of attribution, see e.g. Rid & Buchanan, 2015; Guitton, 2017). Simultaneously, '[d]espite the cross-border nature of cyber threats, states generally dismiss the premise of adversarial relations when addressing international cyber security issues' (Tikk, 2017, p. 152).

In addition, strategization utilizes a number of calculations in evaluating one's own capabilities – most commonly versus the enemy's/ies' strengths and weaknesses. These may be clear-cut calculations of the amount of weapons, but in the cyber domain, where the fog of war is often thicker, they tend to be speculative calculations of probability and risk (e.g. Barnard-Wills & Ashenden, 2012; cf. Kramer, 2009, p. 3, 7; about the overall role of calculation in contemporary warfare, see e.g. Press, 2005; Dillon & Reid, 2009). On the basis of political guidance and the aforementioned calculations, the state and its armed forces then define their objectives in cyberspace and decide upon the ways in which reaching these objectives becomes possible. The main objective commonly sought in both discursive and material practices of militarization is the maintenance and improvement of national security. Next to that, decisions upon actions and evaluation criteria for those actions are taken. The evaluation of the successfulness of the actions is carried out on the basis of the selected criteria, while observing and foreseeing the enemy's/ies' actions and responding to them. When the dynamics of action and counteraction come in, the borderline between strategic and operational decision making begins to blur. Much of the criticism of contemporary efforts to organize national cybersecurity arise from this blurriness and point out that the weighing of operational response over strategic approach causes confusion, inaction, avoidance of responsibility, and reactionary response (e.g. Lehto et al., 2017; 2018).

Regardless of the practical challenges, cybersecurity discourse incorporates militarized strands pondering upon issues such as deterrence, the dominance of attack over defence, (military) cyber power and domain prevalence, cyber weaponry and arms race, cyber war operations and tactics, weapon-counter weapon dynamics, prevention and pre-emption, intelligence, and so forth (e.g. Kramer et al., 2009; Carr, 2012; Katin-Borland, 2012; Kiravuo & Särelä, 2013; Limnell, 2013; Shaheen, 2014; to an extent also Nye 2011). In addition, cybersecurity theorization may take place with reference to classical strategic thinkers (e.g. Hanska, 2013; Greathouse, 2014), the value of whose thoughts is evaluated varyingly. The strengthening of hybrid war discourse, in which cyberwar has often been incorporated, has blurred the already unclear conceptualizations further. This has not prevented, for example, the inclusion of cyber warfare in teaching at national defence universities and/or colleges.

Further techniques of militarization include the rather quantitative or both qualitative and quantitative dimensions of armament and organization. Differing from the traditional proliferation theorizing cyber armament cannot be observed by calculating weapons and making sure that their numbers do not exceed the quotas agreed upon in (dis)armament treaties. This fact has not prevented the use of 'classical arms control playbook' in international dialogue (Tikk, 2017, p. 151). Even if not accepting the calculability of cyber arms, human knowledge, creativity and skill have occasionally been named as the 'actual cyber weapon', for which reason global competition for the best skilled and innovative individuals (most often of 'STEM graduates') is said to be taking place (e.g. Kramer, 2009, p. 8–9; Limnell et al., 2015, p. 141). As a skilled individual can be considered a 'dual-use weapon', contributing to both digitalization enabled prosperity of a nation and its warfighting capabilities, we are hesitant to call the increasing emphasis on ICTs and cybersecurity education and training mere militarization. Digitalization may advance international peace and security as much as it can hinder it. With regard to cyber armament, an additional challenge in estimating the capabilities of different actors is provided by secrecy characteristic to the topic, mutual vulnerability to the same innovations, and speculations regarding actors' unwillingness to use cyber weapons in some situations so that the stage of their cyber military development stays uncertain (e.g. Healey & Grindal, 2013, p. 67; Shaheen, 2014, p. 78; Tikk, 2017, pp. 163–164). Moreover, public defence budgets do not tend to specify investments in cyber military

R&D, for which reason international comparisons remain speculative. The organizational evolution will be addressed in the next section with a focus on US and Dutch developments.

Alongside technologies, the way these technologies are utilized in warfighting are diffusing, as, for example, the relatively wide adoption of information warfare or network-centric warfare concepts testifies. Demchak (2003, p. 308) claims that ‘the global spread of the information warfare concept [alongside related military modernization] differs from established historical patterns of iterative changes in militaries orchestrated by leaders who perceived threats to their regional, technological, or economic security’. States with varying resources and threat environments currently follow the example of a leading state and transform their militaries to suit this concept, because ‘this new form is perceived as legitimate and modern’, that is, it constitutes the contemporary norm (Demchak, 2003, pp. 308–309). Regarding the concept of network-centric warfare, ‘[p]art of the problem lies in identifying exactly how a transformed military will look and fight’ with its new ICTs (Junio, 2012, p. 51). Organization and doctrine are under development – similarly to the cyberwarfare concept. ‘Another part [...] is the puzzling spread of military desires to develop [US like] networked forces’ regardless of their differences, for example, in culture, threat perceptions, geographic situation and regional power dynamics, history, organization, and political objectives (ibid.). According to Junio (2012, p. 67–69), the reasons for this diffusion may be found in technology cultures basing on what ICTs enable and influencing the diffusion process. States being transformed by the concept are highly saturated with ICTs; states that are not may be hindered by other factors, such as resources or domestic politics; and different ICT cultures are developing in interaction with local cultures that either support or restrain the change.

In the following section, we ask about the assumed political and operational, utilitarian value of cyber military capabilities. In exemplifying how the accumulation of national power projection capacity, organizational development and legitimizing manoeuvres have taken place in certain countries, we follow Alexander Wendt’s (1989) framework of accumulation, organizing and legitimizing (military capacity). We consider this framework a useful meter to analyse national cyber proliferation. Our sharp focus on the experiences of the United States and the Netherlands does not suggest that other countries do not possess, or are not developing, cyber military capabilities. On the contrary, for example, Russia and China are considered clever in utilizing proxies, but analyses of their hacking capabilities, computer network operations, signal intelligence, and electronic warfare capabilities would not add value to our conceptual research interest. Credible analyses of the Chinese, Iranian and Russian military cyber, or better information, warfare developments can be found in Inkster (2018), Kania & Costello (2018), Morgus et al. (2019), Martins (2018), and Giles (2016), respectively. The selected examples are considered representative samples of the processes of modernization, securitization and militarization in and of the ICT environment, even contemporary ideal models. Although the contemporary proliferation of cyber military capabilities is still at relatively early stages, some patterns have begun to emerge (Pernik, 2018; Feakin & Weaver, 2019).

Coded arms and armed codes: the military utility of information and communication

Why cyber military capabilities? The development and proliferation of cyber military capabilities seem to mainly follow from instrumental (operational) and institutional imperatives. Cyber military capabilities can simply be regarded as creating better effects or effects in a better way. While the former refers to the combined accuracy and effectiveness of

military action, the latter aims at mainly cognitive-psychological but also paralyzing effects – comparable to physical effects that the employment of cyber capabilities may create. To put it simply, cyber military capabilities are seen as force multipliers increasing effectiveness in the battlefield (USCYBERCOM, 2018; Kerttunen, 2018). Echoing US Cyber Command's conviction, offensive cyber capabilities are argued even to provide 'significant strategic advantages', mainly another option to employ, that is, employment in conjunction with conventional military forces, psychological ascendancy, and usage with almost no casualties (Smeets, 2018).

United Nations Institute for Disarmament Research's (UNIDIR) 2013 report identified 114 countries with national 'cybersecurity programmes'. Despite the report explaining that these national agendas can range anywhere between basic network security and declared offensive cyber capabilities, the number of '114' has in several occasions been taken to represent dangerous militarization of cyberspace, even an arms race. The UNIDIR report goes on to list 47 countries that give 'some role' in national cyber security to armed forces – a number frequently presumed as countries with military cyber capabilities. The report then counts 27 countries having established or planning to establish specific military 'cyberwarfare' entities, of which 17 also comprise offensive military capabilities (UNIDIR, 2013, p. 3–4). More recent analysis (Kerttunen & Tikk, 2019) similarly shows that fewer countries are actually developing employable national cyber military capabilities. The majority of countries are, at least currently, struggling to protect their own networks and information and add a digital layer on to their established military functions. Pernik's (2018; 2019) analysis of the development of national cyber commands implicitly supports this conclusion.

Cyber-electromagnetic activities and means and methods of information warfare are yet being developed and integrated into a full range of military operations. Information and communication technologies have become an elementary part of any human (sic!) activity, war and conflict included. Furthermore, offensive cyber operations and the already-established signal intelligence, electronic warfare and information operations, now with assumingly better effects and better ways, are being employed in on-going armed conflicts (Brose, 2019).

It is essential to observe that the process of creating deployable cyber capabilities – organized, trained and equipped units and teams – is slow. Writing malicious code, the romanticized aspect of capability development, produces the algorithms necessary to create the desired first-level effects, but do not constitute national or military capability. It is erroneous to treat codes as capabilities or capacity for they are, at most, capability elements (de Spiegeleire, 2011). Similarly misleading is to count individual hackers or proxies into sustainable national cyber power or prowess.

The example of the United States testifies to the relatively slow process of national cyber military capacity development. The example also manifests the comprehensiveness and transformative nature of an increasing state-organized power projection capacity. The United States was first to publish national, joint and service level cyber military strategies, doctrines, and manuals. Following the success of the First Gulf War and the conceptual and technological development of the 1990s and early 2000s, the 2006 National Military Strategy for Cyberspace Operations was the first national strategy to focus on cyberspace operations. (Tikk-Ringas, 2016.) The US Cyber Command was established in 2010; a joint doctrine, *Cyberspace Operations* (JP 3–13), was published in 2012 (renewed in 2018); and an Army Field Manual, *Cyber-Electromagnetic Activities* (FM 3–38) came to light in 2014. No other country has been able to achieve this level of conceptualization and organization in cyber military activities; not by 2012, 2014, or 2019. The US has been systematic and

continued developing its cyber military capabilities. In 2014, the then-commander of US Cyber Command and the National Security Agency, Admiral Michael Rogers, called for the development of five capabilities [capability elements] that must exist ‘if cyberspace is to become viable as a military domain’ – namely, defensible network, shared situational awareness, authority and responsibility to act, operational concepts and a command-and-control structure, and trained and employable forces (Pellerin, 2014). The development of those employable units and teams has taken time. The force goal of 133 teams, comprising of circa 5,000 troops, was set in 2009. Initial operative capability was achieved after some three years of concentrated work in October 2016 (DOD, 2016). Full operational capability, with circa 6,200 troops, was achieved in May 2017 (DOD, 2017).

The US has also continued to develop responsive cyber policies. James Lewis (2019) argues that the United States’ cybersecurity policy has changed significantly under the Trump administration. According to him, the key change is a realization that the US’s cyber opponents are unlikely to change their behaviour without the imposition of consequences: the era of President Obama’s ‘legalistic and timid’ approach is over. Instead, the US pursues two parallel avenues: one of ‘persistent engagement’ and another of ‘collective deterrence’ (Lewis, 2019). While the US Cyber Command advocates for continuous and, if necessary, unilateral responses, the Department of State seeks to rally likeminded governments to collective responses, including countermeasures in occasions in which other countries depart from the norms of responsible state behaviour. (USCYBERCOMMAND, 2018; DOS, 2018.)

In the Netherlands, the story of military cyber capabilities can be traced back to the recommendations of international affairs and public international law advisory bodies in 2011 (Pijnenburg Muller, 2019). The *Cyber Warfare Report* (AIV/CAVV, 2011) noted how the employment of ‘operational cyber capabilities’, offensive ones included, can support the core tasks of the Dutch armed forces – namely, the protection of the integrity of the nation and its allies and the promotion of the international stability and legal order (p. 13). Six months later, the first cyber defence strategy was issued. Moreover, the Dutch cyber command become operational in 2017, and the second strategy was issued in 2018. By the 2012 *Strategy*, Dutch politicians explicitly acknowledged the Armed Forces’ view of ‘digital assets as operational capabilities, i.e. as weapons or as intelligence assets, which must be incorporated in the operational capabilities of the armed forces as a whole’ (p. 5). The six focal points to achieve the set objectives included the development of defensive, offensive and intelligence capacities (MOD, 2012, pp. 5–6). The 2018 *Strategie* further emphasized the military operational importance of the cyber domain and digital battle (MOD, 2018, pp. 8–11, 12–13).

By observing the accumulation of national capacity in developing cyber military power, the establishment of cyber military command and units, and the legislative measures made to enable this development, we make a materialistic claim of the ontological status of cyber capability. As cyber military capabilities can indeed be detected and tracked, they can be subjected to national audits, academic investigation and arms control verifications (Tikk, 2017). Paradoxically, the proliferation of national cyber military capabilities offers avenues to try to monitor and influence its development through public and international awareness, debate, and negotiations.

Threats to international peace and security – and other consequences

From the diffusion of innovations/digital militarization discussion briefed earlier in this chapter, we can detect three tendencies problematic for the maintenance of international peace and security. First, when established concepts – such as war, confidence-building

measures and international law – are replaced by their cyber-equivalents (cyberwar, cyber confidence-building measures and voluntary non-binding norms) we end up employing suboptimal measures to secondary issues. This problem manifests in the much-celebrated, and sought-after, United Nations Group of Governmental Experts on ‘Developments in the field of information and telecommunications in the context of international security’ process, which has failed, or has chosen to fail, to seriously address issues of international security (Tikk & Kerttunen, 2018). Secondly, when conflict and escalation are regarded normal, peace and normalcy become abnormal and remain unattended. Thirdly, when the form of conflict and war replaces the nature of conflict and war (see Clausewitz, 1991/1832, 1:1, 28), attention (again) is paid to secondary issues. In sum, all that virtualization, securitization, and militarization create is a fallacy of achievement and investment, which still remain an illusory progress.

The nuances of the diffusion/proliferation of national cyber power projection capabilities are not necessarily tangible or as obvious as in the examples of conventional or even nuclear proliferation. Proliferation, securitization and militarization of ICTs are not necessarily ‘military’ but often ‘civilian’ processes. They are not necessarily employed for military operational purposes either, but are being acquired and used for ‘civilian’ purposes of monitoring, surveillance, and intelligence. Moreover, the previously distinct line between military and civilian authorities, operations, and capabilities has become blurred. This militant move is conceptually, doctrinally, and empirically detectable. Cyberspace is not only bothered by military presences and operations but, perhaps most often and alarmingly, by non-military aggressive and offensive, easily destabilizing and escalatory, activities. Therefore, as in the question of space militarization in the 1950s and 1960s (Heinze, 2001), and in contemporary conflict studies (Mitchell & Hensel, 2011), instead of analysing general and structural conditions of conflict – such as the build-up of military capabilities – attention ought to be directed to the behaviour of states and the issues causing conflictual behaviour. This weighing is more suitable for the purposes of international peace and security. While any given capacity does not necessarily make a state or a government militant, the lack of cyber capabilities does not prevent any government from becoming militant in this field. The West, in particular, has played with an interpretation of collective countermeasures where ‘states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation’ (Kaljulaid, 2019).

Some governments argue that digitalization is dangerous. We argue that becoming militant is dangerous. Not only because of the increased possibility and temptation to employ relatively fast, cheap, and clandestine means of power projection under the established threshold of banned activities, but also, and predominately, because of the transformative power security-heavy politics have over national and societal development. The question is not of too much security but of planting statist, corrupting, and antagonist frameworks on the use of ICTs and advanced technologies instead of promoting trust, cooperation, societal development, and individual welfare and empowerment. For example, by comparing the Norwegian and Dutch cyber military strategies, Lilly Pijnenburg Muller (2019, p. 3) observed that while having rather similar values and objectives, the Norwegians are much more restrained and focused on counter-intelligence than the ‘vocal’ Dutch with their offensive means. We continue this argument by noticing a qualitative difference between modernizing armed forces and becoming cyber militant. The former does not require the latter. Considerations and readiness to project national and military power on-line should be no different from those of off-line. The facts that no cyberwar is going on and the number of actual state-on-state cyber conflicts – incidents and operations – is very low testify that

national security and cybersecurity are predominately pursued by by-default peaceful technical and procedural manners. In addition, according to Joseph S. Nye (2011, pp. 113–122), the ongoing global diffusion of power does not favour centralized responses in cyberspace in general, but require the acknowledgement of a qualitative change in how the state functions as one of the players amongst others.

Nonetheless, the responsive and offensive stand has its supporters. General Paul M. Nakasone, the Commander of the US Cyber Command and Director National Security Agency, explains that '[U]nlike the nuclear realm, where our strategic advantage, or power comes from possessing a capability or weapon system, in cyberspace, it's the *use* [orig. emphasis] of cyber capabilities that is strategically consequential'; the threat of escalation and employment matters less than the actual employment of cyber capabilities and the one who seizes the initiative has the advantage (JFQ, 2019, p. 4). Yet, what if Russians, Chinese, and all other nations possessing or to striving to possess cyber military capabilities would like to seize the initiative as well; not necessarily against the US, but against their neighbours or 'difficult' countries? Security and cybersecurity are needed. Military cyber capabilities are less destructive than conventional capabilities, let alone nuclear weapons. The flickering whisper of better-and-better cyber military capabilities can deafen the voices of normalcy, carefulness, and, yes, peace. Here, the optimists may regard cyber militarization as business-as-before and hope for the fever to eventually normalize.

Yet, to avoid the destabilizing and escalatory lowering of the threshold of power projection, resilience must be promoted prior to responses. Strengthening the national capacity to detect, manage, mitigate, and resolve cyber incidents is the best medicine against the doubt and insecurity that has come to shadow the employment of smart and connected technologies. Currently, popular voluntary non-binding norms, rules and principles may provide guidance, but they cannot solve the fundamentally domestic issues. Any global solution, UN or private sector-centric, binding or non-binding, requires national action and responsibility. True international patching, for example, through confidence-building measures, can help address some of the questions of doubt and insecurity that overt militarization raises.

In addition, we call for increased parliamentary control, national audits, and international tracing of the development of cyber military capabilities, and also of cyber civilian capabilities that are able to project power and cause harm. We claim that this is more than feasible: national cyber capabilities, military or civilian, are not invisible or virtual. On the contrary, they are very material and consume political attention, human resources, and financial means. Methodologically credible and unbiased analysis should be extended to the politics of national and international cybersecurity. Thus far, international and national think tanks and watchdogs have been hibernating or, even worse, uncritically circulating rumours and threat perceptions that support the establishment and conventional truths.

A kick-start in breaking this inertia would be to detect who are setting the cybersecurity agenda, who are allowed to speak, and what can or cannot be expressed in a meaningful and influential manner. To paraphrase Foucault (1984), the order of discourse may reveal a discourse of order. Nationally, we may note that ministries of defence silence, say, ministries of communication or economic affairs. Internationally, we may notice that an agenda of doom dominates over an agenda for development and justice. Moreover, particular ways to speak and to be silent may be promoted. We may also notice cyber operations promoting interpretations of international law that show an emphasis on peace, prevention, and prudence. By opening our eyes and ears, we may notice that not only cybersecurity but also national IT/ICT/e-approaches have been conceptualized and understood within the military vocabulary and logic.

The most obvious dangers of militarization/becoming militant have a simultaneous and dualistic relationship: an increased ability and willingness to project national power in and through cyberspace and a decreased attention to the foundations of sustainable peace and stability, that is, the rule of law (applying to all states equally), the protection of human rights, and fundamental freedoms, as well as development. Furthermore, in the process of becoming militant the controlling, selective and redistributing narrative of national sanity and security becomes a master societal agent of exclusion (Foucault, 1984, p. 109). Rather than reading the international climate to demand and international law to allow responses, let us take the peaceful settlement of disputes as our guiding light.

References

- Advisory Council on International Affairs (AIV) and Advisory Committee on Issues of Public International Law (CAVV) (2011) *Cyber Warfare*. No 77, AIV / No 22, CAVV December. Available from: <https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf> [accessed 22 May 2019].
- Alhanen, K. (2007) *Käytännöt ja ajattelu Michel Foucault'n filosofiassa*. Helsinki, Gaudeamus.
- Arquilla, J. (2003) Patterns of commercial diffusion. In Goldman, E.O. & Eliason, L.C. (eds) *The Diffusion of Military Technology and Ideas*. Stanford, Stanford University Press, pp. 348–369.
- Arquilla, J. & Ronfeldt, R. (1993) Cyberwar is coming! *Comparative Strategy*. 12(2): 141–165. Available from: www.rand.org/pubs/reprints/RP223.html [accessed 21 May 2019].
- Barnard-Wills, D. & Ashenden, D. (2012) Securing virtual space: Cyber war, cyber terror, and risk. *Space and Culture*. 15(2): 110–123.
- Barlow, J.B. (1996) A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation. Available from: www.eff.org/cyberspace-independence [accessed 27 March 2019].
- Božovič, M. (1995) *Jeremy Bentham: The Panopticon Writings*. New York, Verso.
- Brose, C. (2019) The New Revolution in Military Affairs. War's Sci-Fi Future. *Foreign Affairs* (May–June) Available from: www.foreignaffairs.com/articles/2019-04-16/new-revolution-military-affairs [accessed 21 May, 2019].
- Bulletin to the Atomic Scientists (BAS) (2011) Ronald Deibert: Tracking the emerging arms race in cyberspace. Interview. *BAS*. 67(1): 1–8.
- Carr, J. (2012) *Inside Cyber Warfare. Mapping the Cyber Underworld*, 2nd edition. Sebastopol, O'Reilly Media.
- Center for Strategic and International Studies [CSIS] (1998) Cybercrime... Cyberterrorism... Cyberwarfare... Averting an electronic Waterloo. *Global Organized Crime Project*. CSIS Task Force Report. Washington, CSIS.
- Chivvis, C.S. (2017) *Understanding Russian Hybrid Warfare*. Santa Monica, Rand Corporation.
- Clarke, R.A. & Knake, R.K. (2010) *Cyber War: The Next Threat to National Security and What to Do About It*. New York, Harper Collins.
- von Clausewitz, C. (1991/1832) *Vom Kriege*. Köln, Ferd. Dümmler Verlag.
- Deibert, R.J. (2003) Black code: Censorship, surveillance, and the militarisation of cyberspace. *Milennium*. 32(2): 501–530.
- Deibert, R.J. (2017) Cyber-security. In Dunn Cavelty, M. & Balzacq, T. (eds), *Routledge Handbook of Security Studies*, 2nd edition. Abingdon: Routledge, pp. 172–182.
- Demchak, C.C. (2003) Creating the enemy. Global diffusion of the information technology-based military model. In Goldman, E.O. & Eliason, L.C. (eds), *The Diffusion of Military Technology and Ideas*. Stanford, Stanford University Press, pp. 307–347.
- Demchak, C.C. (2011) *Wars of Disruption and Resilience. Cybered Conflict, Power, and National Security*. Athens, University of Georgia Press.
- Demirciogly, M.A. & Audretsch, D.B. (2017) Conditions for innovation in public sector organizations. *Research Policy*. 46: 1681–1691.
- Der Derian, J. (1992) Cyberwar, videogames and the Gulf War syndrome. In Der Derian, J. *Antidiplomacy, Spies, Terror, Speed and War*. Oxford, Oxford University Press, pp. 173–202.
- Dillon, M. & Reid, J. (2009) *The Liberal Way of War. Killing to Make Life Live*. Abingdon, Routledge.
- Dunn Cavelty, M. (2008) *Cyber-Security and Threat Politics. US Efforts to Secure the Information Age*. Abingdon, Routledge.

- Dunn Cavelty, M. (2012) The militarisation of cyberspace: Why less may be better. In Czosseck, C., Ottis, R., & Ziolkowski, K. (eds). *4th International Conference on Cyber Conflict*. Tallinn, NATO CDCE.
- Dunn Cavelty, M. (2020) Cybersecurity between hypersecuritization and technological routine. In Tikk, E. & Kerttunen, M. (eds), *Routledge Handbook of International Cybersecurity*. Abingdon, Routledge.
- Feakin, T. & Weaver, J. (2020) Cyber diplomacy: An Australian perspective. In Tikk, E. & Kerttunen, M. (eds), *Routledge Handbook of International Cybersecurity*. Abingdon, Routledge.
- Finnemore, M. & Hollis, D.B. (2016). Constructing norms for global cybersecurity. *The American Journal of International Law*. 110(3): 425–479. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843913 [accessed 22 May 2019].
- Foucault, M. (2009/1969) *The Archaeology of Knowledge*. Abingdon, Routledge. Translated by A. M. Sheridan Smith.
- Foucault, M. (1984) The order of discourse. In Shapiro, M.J. (ed.), *Language and Politics*. Oxford, Blackwell, pp. 108–138.
- Foucault, M. (1995) Panopticism. In Foucault, M., *Discipline & Punish: The Birth of the Prison*, translated by A. Sheridan. New York, Vintage Books, pp. 195–228.
- Gomez, M.A. & Villar, E.B. (2018) Fear, uncertainty, and dread: Cognitive heuristics and cyber threats. *Politics and Governance*. 6(2): 61–72. Available from: www.cogitatiopress.com/politicsandgovernance/article/view/1279/1279 [accessed 19 May 2019].
- Greathouse, C.B. (2014) Cyber war and strategic thought: Do the classic theorists still matter? In Kremer, J.-F. & Müller, B. (eds), *Cyberspace and International Relations. Theory, Prospects and Challenges*. Heidelberg, Springer, pp. 21–40.
- Green, J.A. (2015) The regulation of cyber warfare under the *jus ad bellum*. In Green, J.A. (ed.), *Cyber Warfare. A Multidisciplinary Analysis*. Abingdon, Routledge.
- Greenstein, S. (2015) *How the Internet Became Commercial. Innovation, Privatization, and the Birth of a New Network*. Princeton, Princeton University Press.
- Giles, K. (2016) *Handbook of Russian Information Warfare*. Rome, NATO Defence College.
- Guitton, C. (2017) *Inside the Enemy's Computer: Identifying Cyber Attackers*. New York, Oxford University Press.
- Hanska, J. (2013) The emperor's digital clothes: Cyberwar and the application of classical theories of war. In Rantapelkonen, J. & Salminen, M. (eds), *The Fog of Cyber Defence*. Helsinki: National Defence University of Finland. Available from: <http://urn.fi/URN:ISBN:978-951-25-2431-0> [accessed 21 May 2019].
- Healey, J. & Grindal, K. (eds) (2013) *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Vienna, Cyber Conflict Studies Association.
- Heintze, H.-J. (2001) Peaceful uses of outer space and international law. In: Bender, W., Hagen, R., Kalinowski, M. & Scheffran, J. (eds) *Space Use and Ethics*. Münster, Agenda, pp. 243–250. Available from: www.space4peace.org/ethics/puosil.htm [accessed 13 June 2019].
- Inkster, N. (2018) *China's Cyber Power*. Abingdon, Routledge.
- Joint Forces Quarterly (JFQ) (2019) An Interview with Paul M. Nakasone. *JFQ*. 92 (1st Quarter), 4–9.
- Junio, T. (2012) Marching across the cyber frontier: Explaining the global diffusion of network-centric warfare. In Costigan, S.S. & Perry, J. (eds), *Cyberspaces and Global Affairs*. Farnham, Ashgate, pp. 51–73.
- Kahn, K.B. (2018) Understanding innovation. *Business Horizons*. 61: 453–460.
- Kaljulaid, K. (2019) President of the Republic at the opening of CyCon 2019. Speech at the NATO CCDCOE conference 'Silent Battle'. Tallinn (29 May). Available from: <https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/> [accessed 11 July 2019].
- Kan, P.R. (2013) Cyberwar to Wikiwar: Battles for cyberspace. *Parameters*. 43(3): 111–118.
- Kania, E.B. & Costello, J.K. (2018) The strategic support force and the future of Chinese information operations. *The Cyber Defense Review*. 3: 1.
- Katin-Borland, N. (2012) Cyberwar: A real and growing threat. In Costigan, S.S. & Perry, J. (eds) *Cyberspaces and Global Affairs*. Farnham, Ashgate, pp. 3–22.
- Keegan, J. (2005/1993) *Sodankäynnin historia [A History of Warfare]*. Jyväskylä, Ajatus Kirjat/Gummerus. Finnish translation by Jouni Suistola.
- Kerttunen, M. (2018) Cyber warfare – from science fiction to reality. *Sicherheit und Frieden*. 36(1): 27–33.

- Kerttunen, M. & Tikk, E. (2019) *A Normative Analysis of National Cyber Security Strategies*. Paris, EU Institute for Strategic Studies.
- Kiravuo, T. & Särelä, M. (2013) The care and maintenance of cyberweapons. In Rantapelkonen, J. & Salminen, M. (2013) *The Fog of Cyber Defence*. Helsinki: National Defence University of Finland, pp. 231–243. Available from: <http://urn.fi/URN:ISBN:978-951-25-2431-0> [accessed 21 May 2019].
- Kramer, F.D., Starr, S.H., & Wentz, L.K. (eds) (2009) *Cyberpower and National Security*. Dulles, Potomac Books.
- Kramer, F.D. (2009) Cyberpower and national security: POLICY recommendations for a strategic framework. In Kramer, F.D., Starr, S.H., & Wentz, L.K. (eds), *Cyberpower and National Security*. Dulles, Potomac Books, pp. 3–23.
- Lehto, M., Limnell, J., Innola, E., Pöyhönen J., Rusi, T., & Salminen, M. (2017) Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi [Finland's cyber security: the present state, vision and the actions needed to achieve the vision]. Publications of the Government's analysis, assessment and research activities 30/2017. Prime Minister's Office, 17.2.2017. Available from: https://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0 [accessed 10th July 2019].
- Lehto, M., Limnell, J., Kokkomäki, T., Pöyhönen, J., & Salminen, M. (2018) Kyberturvallisuuden strateginen johtaminen Suomessa. [Strategic management of cyber security in Finland] Publications of the Government's analysis, assessment and research activities 28/2018. Prime Minister's Office, 29.3.2018. Available from: <https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160717/28-2018-Kyberturvallisuuden%20strateginen%20johtaminen.pdf> [accessed 10th July 2019].
- Lewis, J. (2020) Risk, resilience and retaliation: American perspectives on international cybersecurity. In Tikk, E. & Kerttunen, M. (eds), *Routledge Handbook of International Cybersecurity*. Abingdon, Routledge.
- Libicki, M.C. (2009) *Cyberdeterrence and Cyberwar*. Santa Monica (CA): RAND Corporation. Available from www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf [accessed 21 May 2019].
- Limnell, J. (2013) Offensive cyber capabilities are needed because of deterrence. In Rantapelkonen, J. & Salminen, M., *The Fog of Cyber Defence*. Helsinki: National Defence University of Finland, pp. 213–220. Available from: <http://urn.fi/URN:ISBN:978-951-25-2431-0> [accessed 21 May 2019].
- Limnell, J., Majewski, K. & Salminen, M. (2015) *Cyber Security for Decision Makers*. Edited by Samani, R. Jyväskylä, Docendo.
- Martins, R.P. (2018) Punching above their digital weight: Why Iran is developing cyberwarfare capabilities far beyond expectations. *International Journal of Cyber Warfare and Terrorism*. 8: 2.
- Mitchell, McLaughlin, S. & Hensel, P.R. (2011) Issues and conflict. In Jakobsen, T.G. (ed.), *War: An Introduction to Theories and Research on Collective Violence*. Hauppauge, Nova Science Publishers. Available from: www.saramitchell.org/mhchapter.pdf [accessed 16 June 2019].
- Morgus, R., Fonseca, B. & Green, K. (2019) Are China and Russia on the cyber offensive in Latin America and the Caribbean? A review of their cyber capabilities and implications for the U.S. and its partners in the region. New America Report (26 July). Available from: www.newamerica.org/cybersecurity-initiative/reports/russia-china-cyber-offensive-latam-caribbean/ [accessed 8 August 2019].
- The Netherlands' Ministry of Defence (MOD) (2012) *The Defence Cyber Strategy*. MOD, The Hague.
- The Netherlands' Ministry of Defence (MOD) (2018) *Defensie Cyber Strategie 2018. Investeren in digitale slagkracht voor Nederland*. MOD, The Hague.
- Nye, J.S. Jr. (2011) *The Future of Power*. New York, PublicAffairs.
- Pellerin, C. (2014) Operationalizing cyber is new commander's biggest challenge. *American Forces Press Service* (June 2).
- Pernik, P. (2018) *Preparing for Cyber Conflict: Case Studies of Cyber Command*. Tallinn, International Centre for Defence and Security.
- Pijnenburg Muller, L. (2019) Military Offensive Cyber-Capabilities: Small-State Perspectives. Norwegian Institute of International Affairs, Policy Brief 1/2019.
- Press, D. G. (2005) *Calculating Credibility. How Leaders Assess Military Threats*. Ithaca, Cornell University Press.

- Rantapelkonen, J. & Salminen, M. (2013) *The Fog of Cyber Defence*. Helsinki: National Defence University of Finland. Available from: <http://urn.fi/URN:ISBN:978-951-25-2431-0> [accessed 21 May 2019].
- Rid, T. (2013) *Cyber War Will Not Take Place*. Oxford, Oxford University Press.
- Rid, T. & Buchanan, B. (2015) Attributing cyber attacks. *The Journal of Strategic Studies* 36(1–2): 4–37.
- Rogers, E.M. (2003) *Diffusion of Innovations*, 5th edition. New York, Simon & Schuster.
- Russian Federation (RU) (2010 and 2016a) *The Military Doctrine of the Russian Federation*; (2016b) *Information Security Doctrine of the Russian Federation*.
- Salminen M. (2019) Refocusing and redefining cybersecurity: Individual security in the digitalising European high north. *The Yearbook of Polar Law*. 10: 321–356.
- Shaheen, S. (2014) Offense–defense balance in cyber warfare. In Kremer, J.-F. & Müller, B. (eds), *Cyberspace and International Relations. Theory, Prospects and Challenges*. Heidelberg, Springer, pp. 77–93.
- Singer, P.W. & Friedman, A. (2014) *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, Oxford University Press.
- Smeets, M. (2018) The strategic promise of offensive cyber operations. *Strategic Studies Quarterly*. 2(3): 90–113.
- de Spiegeleire, S. (2011) Ten trends in capability planning for defence and security. *The RUSI Journal*. 156(5): 20–28.
- Stares, P.B. (1985) *The Militarization of Space. U.S. Policy, 1945–1984*. Ithaca, Cornell University Press.
- Tikk, E. (2017) Cyber: Arms control without arms? In Koivula, T. & Simonen K. *Arms Control in Europe: Regimes, Trends and Threats*. Helsinki, National Defence University.
- Tikk, E. & Kerttunen, M. (2018) *Parabasis. Cyber-diplomacy in Stalemate*. Oslo, Norwegian Institute of International Affairs.
- Tikk-Ringas, E. (ed.) (2016) *Evolution of Cyber Domain*. Abingdon, Routledge/IISS.
- United Nations Institute for Disarmament Research (2013) *The Cyber Index. International Security Trends and Realities*. Geneva, UNIDIR.
- United States Cyber Command (USCYBERCOM) (2018) Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command.
- United States Department of Defense (DOD) (2016) All Cyber Mission Force Teams Achieve Initial Operating Capability. Available from: <https://dod.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/> [accessed 7 June 2019].
- United States Department of Defense (DOD) (2017) Cyber Mission Force Achieves Full Operational Capability. Available from: <https://dod.defense.gov/News/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/> [accessed 7 June 2019].
- United States Department of Defense (DOD) *Summary of the National Defense Strategy Sharpening the American Military's Competitive Edge*. Available from: <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf> [accessed 6 June 2019].
- Virilio, P. (2005/1998) *The Information Bomb*. London, Verso.
- Wæver, O. (1995) Securitization and desecuritization. In Lipschutz, R.D. (ed.), *On Security*. Chichester, Columbia University Press, pp. 46–86.
- Wendt, A.E. (1989) *The States System and Global Militarization*. Ann Arbor, University of Minnesota.
- Workman, M., Phelps, D.C., & Gathegi, J.N. (2013) *Information Security for Managers*. Burlington, Jones & Bartlett Learning.
- Yannakogeorgos, P.A. (2009) *Technogeopolitics of Militarization and Security in Cyberspace*. Newark, Rutgers University.

Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

PART II

Challenges to secure and peaceful cyberspace

Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

8

CYBER VULNERABILITY

Brian Martin

New Year's Eve 1999: people around the world have stockpiled supplies in preparation for possible computer breakdowns. The Y2K problem, also called the 'millennium bug', was due to old computer code not being prepared to cope with the change from 99 to 00 in the final two digits of the year. There were many predictions of disaster but, when the time came, nothing much happened. Aside from a few malfunctions, everything operated as usual.

2009–2010: Iranian centrifuges, used to enrich uranium, start spinning out of control, causing them to self-destruct. The cause is initially unknown. Eventually it is traced to a computer worm, called Stuxnet, presumably written to infect Iranian devices, which also infected other industrial computing systems. Where did it come from? Suspects include US and Israeli intelligence services.

2030? EMP weapons are unleashed against several major cities. EMP stands for 'electromagnetic pulse', which is like lightning but with a more sudden surge of energy. The pulse can short-circuit all sorts of exposed electronic devices, causing massive chaos. Transport, manufacturing and communications are jeopardized.

These are three examples of cyber vulnerability, with very different outcomes. For years before 2000, there was extensive publicity about the impending collapse of computer-based systems. There are two ways to understand the potential disaster that didn't happen. One is to give credit to the diligent work of myriads of computer professionals to ensure that code was not vulnerable. By anticipating possible breakdowns and taking appropriate action, disaster was prevented. The other way to understand Y2K is that the risks were greatly exaggerated, to the benefit of firms offering to fix potentially affected systems. Cyber vulnerability is a problem but so is unreasonable alarm about the danger. Real or imagined cyber threats can be framed in ways that change perceptions, shape policy and serve the agendas of individuals and groups (Dunn Cavelty, 2008).

The case of Stuxnet is entirely different (Lindsay, 2013; Zetter, 2014). It remains shrouded in secrecy, punctured by only a few exposés. What the episode revealed is that computer malware can be used in offensive mode, to interrupt and possibly control computer systems. The existence of Stuxnet shows that it is probably possible to use code to infect enemy communication, banking, medical and a host of other systems. Some would say that if this is possible, then it is likely that spy agencies are preparing to use such code and to defend against it. But because of the secrecy involved, it is unlikely that civilian operations are being protected.

The phenomenon of the nuclear electromagnetic pulse (EMP) is known due to a few high-altitude nuclear tests in the 1950s and 1960s. That was long before the full flowering of the microelectronics revolution that has made everyday operations highly dependent on sensitive equipment. Scientists can calculate the possible effects of an electromagnetic pulse (Lerner, 1981; Wik et al., 1985), but the dangers seem not to influence civilian planning. Even without EMP, the use of nuclear weapons would cause massive disruption to communication and other infrastructures. In recent years, militaries in several countries have worked on developing EMP weapons, with a smaller range, that can be carried by missiles or even in a suitcase. They are also developing and refining methods for deliberate disruption of urban infrastructure, which includes electricity grids, water supplies, sewage treatment systems, transport links, and fuel supplies; cyberwarfare is just one aspect of a wider targeting of facilities and networks vital for urban survival (Graham, 2011).

In the next section, several types of technological vulnerability are outlined. Then, communication vulnerabilities are examined with special attention to different perspectives, in particular the perspective of a repressive government and that of an opposition movement. (Cybercrime is not addressed here because it is not centrally about communication.) Following this are three sections addressing illustrative case studies: the shutdown of the Internet in Egypt in 2011; Edward Snowden's leaks; and struggles over encryption. The final section points to radical ways of addressing vulnerabilities.

Technological vulnerability

Communication systems are vulnerable to breakdown, interruption, disruption and takeover, namely impacts that cause the systems to operate otherwise than designed. These vulnerabilities can generically be called technological, with "technology" interpreted in the sense of including artefacts and associated human and social systems. For example, the technological system of radio includes broadcasting equipment, receivers, personnel, operating procedures and manufacturing processes, among others. Thus, technological vulnerability can involve failures in equipment, in design and use. Typically, in complex systems, vulnerabilities involve sets of linked weaknesses, often in combinations not foreseen (Perrow, 1984).

Although technological vulnerability commonly is multicausal, it is nevertheless useful to point to different areas in which weaknesses can occur. Here is one classification.

- Equipment breakdowns. A circuit malfunctions; there is a power outage; computer code is corrupted due to a physical cause; a storm destroys facilities. Equipment breakdowns are the most obvious source of vulnerability and therefore usually prepared for most comprehensively with checks, back-ups and alternative systems. The more common the breakdown, the more likely it will be anticipated and prepared for. Extremely rare events are the most worrisome. If a contingency has not occurred in a lifetime, memory of the risk may be lost. This happens with natural disasters: when earthquakes are rare, buildings may not be designed to withstand them (Muir-Wood, 2016). Then there are disasters for which there is no precedent. The Fukushima nuclear power plant failure is an example.
- Human error. Humans make mistakes, and mistakes are more common when people are tired, ill, overloaded, unmotivated, poorly managed or caught up in interpersonal clashes. A cable is installed incorrectly; a message is misinterpreted; a signal is overlooked; an incorrect instruction is transmitted; a roster is poorly designed. Human error, like equipment breakdowns, can be anticipated, and sometimes prevented or worked

around, for example by using checklists, auditing, back-ups, and the like. Typically, human failures are intertwined with the design and operation of systems, so that blaming one or the other is misleading. The Chernobyl nuclear accident is an example. The design of the Soviet RBMK nuclear power plant created a number of vulnerabilities not present in other reactor types, and operators were able to turn off safety systems for a test that went disastrously wrong.

- Surveillance. Information about or contained in cyber systems can be obtained illicitly by outsiders, for example by foreign or domestic intelligence agencies. Successful surveillance exploits vulnerabilities in systems, which can be linked to technical or human weaknesses in security systems. Governments and private companies engage in various types of covert information gathering, for example targeting hostile powers during wartime or allied countries for their commercial secrets or political conversations. Most notoriously, the US National Security Agency has been carrying out monitoring of global communications for decades.
- Information exposure. Whereas surveillance involves gathering of information, exposure makes information available to wider audiences, sometimes to the general public. Whistleblowing – speaking out in the public interest – is a type of information exposure. Leaking of information can be considered anonymous whistleblowing, the most prominent example being Edward Snowden’s revelations (discussed below). Organization leaders usually try to prevent leaks, at least from those lower in the hierarchy (Pozen, 2013), and punish leakers, but members of the public may welcome the leaking of information, for example when it shows criminal or unethical behaviour. Furthermore, when there is serious organizational dysfunction, leaking can serve a restorative function, exposing corruption before it causes further damage.
- Sabotage, external. Cyber systems are vulnerable to attack. Potential external attackers include hackers, hactivists, crackers, criminals and government agencies (Wright, 2017, p. 213). A government may seek to break into a communication system in order to destroy or corrupt information. There are some independent script-kiddies and hackers who break into systems for the challenge, amusement, criminal gain or simply to wreak havoc. Probably more commonly, governments use hackers as proxies for this purpose. Non-state terrorists use violence to send messages to audiences, with the mass media as carriers of the messages (Schmid and de Graaf, 1982). With this picture of terrorism, covert sabotage of communication systems might be used to destroy or interfere with manufacturing, power, water or other systems. Whether this is attractive depends on whether the effort required is much greater than when using more direct physical methods, for example explosives.
- Sabotage, internal. Just as important as external attack is sabotage from insiders, which can involve destroying or altering code, or setting up vulnerabilities for later exploitation. Also possible is internal sabotage for criminal or revenge purposes. The possibility of internal sabotage can pose a perplexing security dilemma. In order to prevent insiders from doing damage to highly sensitive systems, governments and militaries institute close screening of employees, for example with access to information on a need-to-know basis. However, the siloing of systems reduces the effectiveness of organizations: information may not be available to those who need it. In essence, the dilemma is finding the right balance between zero sharing, in which no one knows what anyone else knows, and complete sharing, in which information is available to anyone.
- Organizational and political struggles. Cyber systems are the product of both technical considerations and political pressures, with ‘political’ referring generically to the

exercise of power. For example, phone systems are shaped by economic pressures, social expectations, prior infrastructure and the influences of privileged groups. Engineers, technicians and users can influence the uptake of technologies and their vulnerabilities. The level of security obtained depends crucially on organizational culture. When workers are dissatisfied, the result may be inadvertent or intentional shortcomings in systems.

- War. In wartime, cyber systems are crucial and hence are prime targets. A variety of attacking techniques can be deployed, including physical destruction, sabotage, surveillance and black operations (such as fake broadcasters). Systems can be defended by back-ups, greater security and having alternative methods for accomplishing tasks.

There is both a cross-fertilization and a tension between designing systems for war and for peacetime. Cross-fertilization occurs when practices in one domain are taken up in another. A famous example is the military origins of the Internet. Tension occurs when practices in one domain are undermined by those in another, such as when encryption for civilian transactions is compromised by government-sponsored back doors.

Whose security?

In some discussions, the implicit assumption is that security is from the perspective of government, the military or sometimes large companies. In addition, security is assumed to be a good thing. These assumptions need to be questioned.

In wartime, cybersecurity – encompassing information security more generally – is paramount for each side in the conflict. Typically, enemies seek to breach or undermine their opponents' systems. Cybersecurity is good for *us* but not cybersecurity for *them*. This basic point has ramifications for every type of technological vulnerability. Militaries try to prevent or prepare for breakdowns of their own systems while doing what they can to foster breakdowns in the enemy's systems. Preventing sabotage of one's own systems is a key goal, and so is exploiting, denying and damaging enemy systems.

Cybersecurity is also important to others besides governments, militaries and large companies. Individuals – citizens, customers, patients and others – have an obvious stake in the security of communication and information systems. The main difference is that individuals have little capacity for making policy decisions about research, investment and implementation. Nevertheless, the collective choices of individuals can have consequences. For example, when more individuals choose highly secure applications, this encourages designers and companies to cater for the resulting demand, the result being that surveillance becomes more difficult.

An important perspective to consider is that of civil society groups, including clubs, professional organizations, churches, trade unions and environmental groups. Some such groups have only a limited concern about security, for example wanting to protect the privacy of members and to guard against fraud. Others, though, need to protect against adversaries. For example, trade unions may be concerned about surveillance of their members by employers, given that many employers monitor their employees' email and use of social media. Groups seeking to expose corrupt police might need to be prepared for disruption or being framed through false messages and manufactured misdeeds.

By looking at cybersecurity from the perspectives of a number of different groups, it is possible to observe that concerns sometimes differ and occasionally are directly contradictory, in the sense that one group's actions undermine the security of another's. This can be illustrated by a schematic breakdown of cybersecurity issues for two directly opposed groups:

a government and an opposition movement. The government might be a repressive one, such as Russia or China, or an ostensibly more liberal one, such as the United States, that has repressive elements. Table 8.1 lists technological vulnerabilities for the government and Table 8.2 those for the opposition movement.

The most striking difference between these two sets of vulnerabilities relates to what is called sabotage. The repressive government seeks to control and subjugate the opposition movement, and to this end tries to monitor the movement's communications and perhaps to corrupt or destroy the movement's information systems or even to threaten, arrest or kill opponent members. Each of these actions is a distinct vulnerability for the movement. If the government is engaged in a war with an external enemy, this provides a pretext for declaration of martial law and repression of internal opposition movements.

It would be possible to make general observations about the similarities and differences in technological vulnerability for governments, militaries, companies, civil society groups and others. However, initially more insights may be gained through looking at particular episodes

Table 8.1 Communication vulnerabilities for a government with repressive elements

<i>Type of vulnerability</i>	<i>Examples</i>	<i>Examples of responses</i>
Equipment breakdowns	Electricity outages	Redundant systems
Human failure	Programming error	Checks; redundant systems
Surveillance	Surveillance by a foreign power	Firewalls; encryption
Information exposure	Whistleblowing; leaking	Secrecy laws; reprisals
Sabotage, external	Disruption by a foreign power	Firewalls; encryption
Sabotage, internal	Intentional disruption by an employee	Screening of employees; need-to-know protocols
Organizational struggles	Strike by employees	Better wages; arrest of strike leaders
War	Destruction by bombing	Redundant systems

Source: Author's compilation

Table 8.2 Communication vulnerabilities for an opposition movement to a repressive government

<i>Type of vulnerability</i>	<i>Examples</i>	<i>Examples of responses</i>
Equipment breakdowns	Electricity outages	Redundant systems
Human failure	Programming error	Redundant systems
Surveillance	Surveillance by government	Encryption; non-digital communication
Information exposure	Media stories based on information from infiltrators or surveillance	Screening of members; media management
Sabotage, external	Government confiscation of devices; arrests	Encryption; decentralized leadership
Sabotage, internal	Disruption by infiltrating government agents	Monitoring of new members
Organizational struggles	Disputes between rival movement organizations	Methods for mediation
War	Arrests; martial law	Decentralized leadership

Source: Author's compilation

or issues, and this is the approach here. Several striking instances in which cybersecurity has been breached – at least from some groups’ perspectives – will be used to highlight contrasting perspectives.

The Internet in Egypt, 2011

In December 2010, a Tunisian street-seller felt he had been unfairly treated by authorities and immolated himself in protest. This action triggered an upsurge of protest against Tunisia’s repressive government and within a few weeks the popular uprising – unarmed – overthrew the government. The Tunisian popular campaign inspired government opponents in several other Arab countries. One of them was Egypt, where dictatorial rule had been in place for decades, and Hosni Mubarak was a ruthless ruler. The grassroots uprising in Egypt was in part fostered by a Facebook page, ‘We are all Khalid Said’, set up in memory of a young man beaten and killed by police.

The Facebook page was managed by Wael Ghonim, whose hid his identity, knowing that if his name was known to authorities, he and his family would be targets for arrest, torture and murder (Ghonim, 2012). This illustrates a common divergence in security. From the point of view of the Egyptian authorities, Ghonim was a criminal or traitor or troublemaker. The security of the regime depended on being able to identify and arrest him. From the point of view of the popular resistance to the regime, Ghonim was an inspiration, indeed a hero. Security from this perspective meant being able to express opposition without repression from the authorities.

Next consider the role of Facebook, normally seen as a social platform. However, in the context of a repressive government such as Egypt’s in early 2011, Facebook was a convenient tool for resistance, allowing messages to be posted. Facebook subsequently introduced a policy of requiring users to verify their identity, in order to overcome the misuse of the platform by creators of fake profiles. However, in Egypt 2011, anonymity was vital to the continued role of the “We are all Khalid Said” page in the resistance to the regime. The page was rescued from takedown by a sympathiser, living outside Egypt, who put her name to it despite the personal risk (Tufekci, 2017, pp. 141–142).

The security of the government could have been enhanced by being able to access Facebook information. So, between Facebook and the Egyptian government, there were conflicting security interests. To maintain its credibility, Facebook needed to appear to be independent of government, thus enabling it to be used for challenges to the government. If Facebook were thought to be collaborating with the government, then opposition groups would simply shift to another platform.

The Egyptian government, in response to the rapid mobilization of resistance, took a drastic step: on 28 January 2011, it shut down all electronic communications (mobile phones, the Internet, messaging services), thereby demonstrating a potential but seldom exploited vulnerability. Although the Internet shutdown hindered the capacity of regime opponents to organize, they were able to use various workarounds to communicate with each other and with supporters outside the country. The shutdown had several counterproductive effects for the government. First, it meant that everyone heard about the uprising: many previously had not, due to the regime’s control of the mass media. Second, it disrupted businesses and government operations across the country, thereby alienating wide sectors of the population that otherwise might have remained indifferent to the political conflict. Third, many citizens in Cairo and elsewhere, deprived of information about political affairs, went out on the street

to find out what was happening, and some of them ended up joining the protests. Within a few days, the government restored services.

The Egyptian Internet shutdown provides a lesson for challengers to governments about the choice of communication systems. One approach is to set up a dedicated resistance channel, with its own protocols and technology. However, a dedicated channel is vulnerable to disruption that targets only the challengers, whether the disruption is engineered by government or other political opponents. A different approach is to use mainstream communication systems such as Facebook. That has the advantage that disrupting the challengers' communication channels also disrupts many uninvolved individuals and groups, potentially alienating them. This general conclusion requires qualification: each communication channel needs to be evaluated for its own security features.

It should also be noted that repressive governments have learned from their engagements with challengers (Dobson, 2012). The Egyptian government, and others, are now more aware of the role of social media in enabling opposition mobilization and are prepared to counter it with techniques such as overloading social media with propaganda, spreading rumours, questioning the authenticity of claims about government abuses, and harassing social media leaders (Tufekci, 2017). These methods constitute a new sort of vulnerability of communication systems.

'Snowden'

The US National Security Agency runs a massive data collection operation, seeking to obtain nearly all electronic communications, including phone calls and email messages. It has the capability of scanning this vast body of data for keywords, thus enabling tracking of actual or potential terrorists, and much else. The NSA surveillance operates in conjunction with agencies in Australia, Britain, Canada and New Zealand in the so-called Five Eyes arrangement.

The NSA is far larger than the more well-known Central Intelligence Agency. For many years, the NSA, as well as its counterparts in Australia, Britain, Canada and New Zealand, were so secret that even their existence was hidden from public view. The NSA's operations are an evolutionary development from earlier monitoring efforts, including British secret preparations for rule following nuclear war (Campbell, 1982; Laurie, 1970).

From the point of view of the NSA and related agencies, cybersecurity implies protection of its own operations (including its surveillance and disruptive operations), which are part of US government efforts to maintain security against foreign and internal threats. However, NSA monitoring and surveillance are a direct threat to the cybersecurity of every person, company and government whose communications are intercepted. This is a clear example of how security for one group means insecurity for another.

The existence of NSA operations was exposed through investigative scrutiny (Bamford, 1982). A major exposure of the details of the Five Eyes operation was by Nicky Hager, a New Zealand activist who obtained information from many workers at the country's two eavesdropping stations, eventually being able to extract details such as a floor plan despite never having visited the stations. Hager's book *Secret Power*, published in 1996, became well known in circles concerned about operations of spy agencies. In 1998, Steve Wright, drawing on work by Hager and Duncan Campbell, wrote a report for the European Union that drew attention to the Five Eyes' Echelon spying operation. This EU report brought extensive media attention to the massive state surveillance (Wright, 2005).

In 2013, Edward Snowden, an NSA contractor, released to the *Guardian* a large number of internal NSA documents revealing its extensive data collection system. Snowden's revelations generated immense international publicity (Greenwald, 2014; Gurnow, 2014; Harding, 2014). Several factors explain the much greater attention to Snowden's information than to prior exposés. First, he was an insider and thus had greater credibility. Second, he released NSA documents, which had greater credibility than inferences by outsiders like Hager. Third, he teamed up with credible journalists and mass media outlets, so that the leaked information had the greatest possible impact. The media connection had the additional effect of encouraging journalists to learn much more about government surveillance of digital communications. In the furore, the existence of earlier exposés was usually overlooked.

The Snowden leaks and prior exposés starkly show that different groups can have contrary cyber vulnerabilities. The NSA sought to maintain the secrecy and hence security of its own operations; Snowden broke through the secrecy and thereby potentially compromised the NSA's ability to continue to gather worldwide electronic communications unhindered. Companies, foreign governments, NGOs and citizens sought to maintain the security of their communications; Snowden revealed that this security had been being breached and provided the incentive, for some, to use methods to circumvent NSA surveillance.

Encryption struggles

Predating electronic systems, there has long been a struggle between citizens and governments about the security of information and communication. In the early days of the British postal system, the monarch's agents would open mail. Naturally, this was unwelcome to those wanting their messages to be confidential. This led to pressure for a secure postal system, which involved operating principles and expectations in countries around the world (Joyce, 1893). Nevertheless, at times governments attempt to intercept and monitor letters, especially during wartime (Fowler, 1977). One method has been to photograph envelopes sent to particular addresses without trying to read the enclosed letters, foreshadowing the collection of metadata.

In the cyber era, the struggle between sender-receiver secure communication and the desire of governments (and some others) to intercept or monitor messages has continued, with several manifestations. One method to facilitate snooping is to install backdoors in communication devices. In the 1990s in the US, there was a major struggle over the Clipper chip, a proposed microchip to be installed in communication equipment that would allow the US government access to messages (Gurak, 1999). This same struggle continues in a variety of other guises, including public-private key encryption such as PGP and the Tor browser designed to prevent collection of metadata (Landau, 2017).

The details are less important here than the general point that when one group wants to monitor messages of those they see as dangers or opponents, the targeted group may feel threatened and want to prevent this monitoring. An example is governments and militaries seeking state security by means that undermine the communication security of others. However, there are many groups seeking to monitor others, and the ethical and practical implications are wide-ranging (Wright, 2015).

Conclusion

When thinking of the vulnerabilities of information and communication systems, breakdowns often come to mind: component failures, power outages, natural disasters and

unintentional human error that cause interruptions to normal service. The more common the type of failure, the more likely it is to be anticipated, so engineers put a priority on the reliability of components and on building back-up systems. Natural disasters are rare but, in many cases, taken into account. These sorts of vulnerabilities are also 'common' in the sense that everyone has a stake in minimising them. The main constraints are technical and financial.

It is much more challenging to deal with other kinds of vulnerabilities that are less predictable and more dynamic. They are the ones caused by intentional human actions: sabotage by external agents or by insiders, the by-products of organizational struggles, and war. Crackers, for example, seek to break into computer systems for hostile purposes. Although the possibility of such cracking is recognized, it is hard to predict when and how it will occur, because players on both sides of this game of offence and defence are trying to outwit each other. This is also what makes cracking versus anti-cracking a dynamic process. As one set of defences is deployed, attackers explore different modes of attack.

In the case of warfare, the game of cyberattack versus cyberdefence becomes more symmetrical: each side tries to compromise enemy systems while defending its own. In practice, this apparent symmetry may be one-sided, for example in struggles between low-tech insurgents versus high-tech counterinsurgency operations. In the case of drone attacks, the insurgents primarily defend, for example by avoiding electronic communication or switching phones, and have limited capacity to intercept or disrupt the communications of the attackers.

The issue of cybersecurity thus involves two different sorts of vulnerabilities: those that are accidental (breakdowns, human error) and those that are intentional (sabotage, warfare). Discussions of security typically focus on what might be called defence, namely how to make systems more secure. This draws attention away from the intentional causes of insecurity. To put it another way, threats to security are 'naturalized', namely assumed to exist as part of nature or human society, so the challenge becomes adapting to circumstances that are treated as inevitable. To question the assumption about the inevitability of threats opens the door to some other methods of promoting security.

In warfare, the enemy's cyberattacks are the immediate source of vulnerability, so one option is to neutralize the enemy's capacity for attack, for example by destroying equipment or killing personnel. Another option, mainly for insurgents, is to use communication methods that do not rely on digital technology. A quite different approach is to not go to war in the first place. Here, a few examples of this more structural approach to vulnerabilities are outlined.

Managers often see whistleblowing as a threat, as in the cases of Chelsea Manning and Edward Snowden. The usual responses are to make whistleblowing more difficult, to stigmatize whistleblowers and to subject them to severe penalties with the aim of discouraging others from following their example. An alternative approach is to remove the reasons for employees to blow the whistle to public audiences. This means not undertaking actions that are seen by members of the public, and by some employees, as unjust. Manning's leaks were triggered by the wars in Afghanistan and Iraq, including killing of civilians. To prevent a Manning-type disclosure, there should have been no invasions of Afghanistan and Iraq. Given the enormous public opposition to the invasion of Iraq, and the lack of justification for it in international law, the incentive to speak out is obvious enough. Similarly, Snowden decided to leak due to his concerns about massive surveillance of citizens, concerns shared by many members of the public. So one "solution" to Manning-and-Snowden-style breaches of security is not to launch illegal wars and not to maintain massive covert surveillance of citizens.

Consider the possibility of cyber intrusions into nuclear power plants with the aim of triggering a major accident (Soltanieh and Esmailbagi, 2017). A long-term solution is to eliminate nuclear power by promoting energy efficiency and renewable energy sources.

It is important to question the assumption that cybersecurity is necessarily a ‘good thing’. The word ‘security’ has a positive connotation, which is one reason why ‘national security’ is so readily used to justify actions that may be unsavoury, dangerous and/or illegal. National security – and the associated cybersecurity – has been used as a cover for building massive military machines, curtailing civil liberties, assassinating foreign leaders and torturing opponents. So when talking about cybersecurity, it always needs to be asked, ‘for what purpose?’ For example, the great firewall of China is a form of cybersecurity for the Chinese government but at the same time a gross violation of free communication for the Chinese people.

Defenders of systems of secrecy and surveillance can argue that curtailing freedoms is an unfortunate side effect of the more important task of protecting society against foreign and internal enemies. This assumes there are no alternatives. It can be argued that much secrecy is unnecessary (Horton, 2015). Rather than undertake massive spying on citizens, one option is open source intelligence, relying on information that is freely available (Stalder and Hirsch, 2002). Another, more radical, option is what is called publicly shared intelligence, in which independent intelligence enterprises receive information from members of the public and, crucially, openly publish their reports, which thus become available for scrutiny and improvement. The example of the Shipping Research Bureau, which tracked ships trying to break the embargo on trade with South Africa under apartheid, provides a precedent: the Bureau’s reports were more accurate than those of the Dutch intelligence service (de Valk and Martin, 2006).

These examples are intended not as definitive options but rather to emphasize the point that most discussions of cybersecurity do not question the need for greater security and do not explore options outside the usual template of security versus threats. Removing or reducing the threats, rather than defending against them, should be an option.

The electromagnetic pulse, noted at the outset of this chapter, is a rarely considered vulnerability of systems based on microelectronics. One mode of defence is providing protection for crucial circuits, for example via a Faraday shield. Another option is to promote disarmament, because when there are no nuclear or other EMP weapons there is no danger. Of course, disarmament, like other political solutions such as fostering of human rights, will not occur overnight. But it can be put on the agenda for a long-term effort to foster cybersecurity that serves human interests.

References

- Bamford, J. (1982) *The Puzzle Palace: A Report on America’s Most Secret Agency*. Boston, Houghton Mifflin.
- Campbell, D. (1982) *War Plan UK: The Truth about Civil Defence in Britain*. London, Burnett.
- de Valk, G. & Martin, B. (2006) Publicly shared intelligence. *First Monday: Peer-reviewed Journal on the Internet*. 11(9). Available from: <http://firstmonday.org/ojs/index.php/fm/article/view/1397/1315> [accessed 10 January 2019].
- Dobson, W.J. (2012) *The Dictator’s Learning Curve: Inside the Global Battle for Democracy*. New York, Doubleday.
- Dunn Cavelty, M. (2008) *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Abingdon, Routledge.
- Fowler, D.G. (1977) *Unmailable: Congress and the Post Office*. Athens, GA, University of Georgia Press.
- Ghonim, W. (2012) *Revolution 2.0*. London, Fourth Estate.
- Graham, S. (2011) *Cities under Siege: The New Military Urbanism*. London, Verso.

- Greenwald, G. (2014) *No Place to Hide, Edward Snowden, the NSA and the Surveillance State*. London, Hamish Hamilton.
- Gurak, L.J. (1999) *Persuasion and Privacy in Cyberspace: The Online Protests over Lotus MarketPlace and the Clipper Chip*. New Haven, Yale University Press.
- Gurnow, M. (2014) *The Edward Snowden Affair: Exposing the Politics and Media Behind the NSA Scandal*. Indianapolis, Blue River Press.
- Hager, N. (1996) *Secret Power: New Zealand's Role in the International Spy Network*. Nelson, Craig Potton.
- Harding, L. (2014) *The Snowden Files: The Inside Story of the World's Most Wanted Man*. London, Guardian Books.
- Horton, S. (2015) *Lords of Secrecy: The National Security Elite and America's Stealth Warfare*. New York, Nation Books.
- Joyce, H. (1893) *The History of the Post Office from its Establishment Down to 1836*. London, Richard Bentley and Son.
- Landau, S. (2017) *Listening In: Cybersecurity in an Insecure Age*. New Haven, Yale University Press.
- Laurie, P. (1970) *Beneath the City Streets*. London, Penguin.
- Lerner, E.J. (1981) Electromagnetic pulses: Potential crippler. *IEEE Spectrum*. 18(5): 41–46.
- Lindsay, J.R. (2013) Stuxnet and the limits of cyber warfare. *Security Studies*. 22: 365–404.
- Muir-Wood, R. (2016) *The Cure for Catastrophe: How We Can Stop Manufacturing Natural Disasters*. New York, Basic Books.
- Perrow, C. (1984) *Normal Accidents*. New York, Basic Books.
- Pozen, D.E. (2013) The leaky leviathan: why the government condemns and condones unlawful disclosures of information. *Harvard Law Review*. 127: 512–635.
- Schmid, A. P. and de Graaf, J. (1982) *Violence as Communication: Insurgent Terrorism and the Western News Media*. London, Sage.
- Soltanieh, A.A. and Esmailbagi, H. (2017) Security of cyber-space in nuclear facilities. In Ramírez, J.M. & García-Segura (eds), *Cyberspace: Risks and Benefits for Society, Security and Development*, pp. 265–274. Cham, Switzerland: Springer.
- Stalder, F. and Hirsh, J. (2002) Open Source Intelligence. *First Monday*. 7(6). Available from: <http://firstmonday.org/ojs/index.php/fm/article/view/961/882> [accessed 10 January 2019].
- Tufekci, Z. (2017) *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven, Yale University Press.
- Wik, M. et al. (1985) URSI factual statement on nuclear electromagnetic pulse (EMP) and associated effects. *International Union of Radio Science Information Bulletin*. 232: 4–12.
- Wright, S. (2005) The Echelon trail: An illegal vision. *Surveillance & Society*. 3(2/3): 198–215.
- Wright, S. (2015) Watching them: watching us – where are the ethical boundaries? *Ethical Space: The International Journal of Communication Ethics*. 12(3/4): 47–57.
- Wright, S. (2017) Mythology of cyber-crime – insecurity & governance in cyberspace: some critical perspectives. In Ramírez, J.M. & García-Segura (eds), *Cyberspace: Risks and Benefits for Society, Security and Development*, pp. 211–227. Cham, Springer.
- Zetter, K. (2014) *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York, Crown.

9

ENSURING THE SECURITY AND AVAILABILITY OF CRITICAL INFRASTRUCTURE IN A CHANGING CYBER-THREAT ENVIRONMENT

Living dangerously

Vytautas Butrimas

Introduction

STUXNET, the first state-developed cyber weapon, a computer code capable of producing physical/kinetic effects on the target device or system, used to attack the critical infrastructure of another state, was a turning point in the security of cyberspace. Cybersecurity professionals understood that the most sophisticated cyber-attacks now extended to the engineering behind the technologies used to support the operations of critical infrastructure. As Langner (2016) has concluded, ‘Sophisticated attackers go after your engineering systems ... and do not need on-line access’.

In short, clear dangers were threatening the very technical foundations that support the modern economy and well-being of modern societies. The year 2017 may be remembered as another milestone for the security of critical infrastructure. That was the year when cyber thieves stole and sold on the market weaponized malware stolen from a government which was later obtained and modified by another government for use against another government. A new malignant ecosystem was establishing itself in cyberspace. These increasingly serious threats to critical infrastructure emanating from cyberspace were not matched with mitigating measures from the international security policymaking community. Perpetrators saw no reason to moderate their malicious cyber activities and seemed increasingly willing to risk damaging property and hurting people. This chapter reviews a recent sampling of the relevant cybersecurity events, the unsuccessful attempts made by the policy sector to address them and their implications. It concludes with proposals to address these unsettling and dangerous trends in the fields of critical infrastructure protection and international cybersecurity policy.

New threats from the shadows of cyberspace

At the end of the Soviet era one of the fears in the West was that in the chaos that followed some of the former USSR's nuclear weapons would fall into the wrong hands. This did not materialize with nuclear but apparently did happen with state made cyber weapons. Reports came out in 2016 and early 2017 about the theft or leaks of state developed malware, which were being sold on the Internet (Amir, 2016). A group of hackers calling themselves the 'Shadow Brokers' claimed that they were able to steal weaponized government malware from the 'Equation Group', another clandestine entity associated with the work of a government intelligence agency (Gilbert, 2015). It was only a matter of time before this stolen state cyber arsenal was adapted by someone else and used. Evidence appeared on Friday May 12, 2017 when many users of computers and systems saw ransom notes on their screens informing them that their data was encrypted and if they would have to pay a ransom in Bitcoin to retrieve it. This ransomware outbreak called 'WannaCry' caused disruptions in services across a variety of sectors (Goodin, 2017). The ransom message appeared on viewing screens at railroad stations and even in hospital emergency rooms (Suiche, 2017). The fear raised also indirectly caused what resulted in a 'Denial of Manufacturing,' causing some automobile plants to shut down as a precaution (Weiss, 2017). One colleague who was working for a national power distribution company told me that on that Friday 'no employees went home'. Instead, they spent time double-checking their critical systems for the presence of the infection. The fear, uncertainty and doubt generated in the industrial sector provoked these precautionary actions even though no malware may have been present. However, the precautions taken were well founded. The malware made use of a government produced and later stolen code called 'Eternal Blue' that exploits an old vulnerability present in Windows operating systems (OS). It is not unusual to find in the industrial sector older or unpatched Windows OS used in industrial control systems and connected devices. While Microsoft distributed the patch for this vulnerability earlier, many in the manufacturing sector, especially those operating real-time critical systems, could not easily set aside the time to shut down a plant in order to implement the patch. This was especially true for sites that for reasons of industrial risk do not patch their software. This is why some industrial operators were anxious about the potential harm from WannaCry.

Another of the implications of WannaCry was the possibility of using state malware for money-making purposes. Less skilled cybercriminals or hackers could now use a state's cyber weapon as a means to get huge ransom money from a manufacturing facility, water treatment plant or power utility. Variations of the WannaCry malware attacking systems from cyberspace followed. One of the ransom malware variants of WannaCry called 'NotPetya' seems to have been planted in and spread from Ukraine (Schwartz, 2017). Serious operational disruptions occurred worldwide. Affected systems were found in unlikely places from a candy factory in Australia to Russia's biggest oil producer, Rosneft to Danish shipping company Maersk. The appearance of variants of this malware in quick succession indicated to at least one cybersecurity industry opinion leader that this activity was now recognized by cybercriminals as a lucrative business (Schwartz, 2017). Surprisingly it caused serious financial loss to innocent victims caught in the cross-fire, namely Maersk whose CEO claimed that the NotPetya infection that apparently targeted ICS in Ukraine cost Maersk 300 million of dollars in damages (Crozier, 2018). These losses illustrate the 'collateral damage' that can follow targeted cyber-attacks.

Later analysis of NotPetya indicated that the creators were not cyber criminals motivated by financial gain. While the function of encrypting or erasing data on hard drives was being

used the ransomware function was not fully developed or would not even work (Kirk, 2017). In other words, the attackers didn't care if the ransom payment module worked or not! The creators focused more on making sure this killing malware would spread quickly and as widely as possible (Greenberg, 2018). The motive behind using malware to cripple a system and make it look like a ransomware attack is far more sinister and perhaps points to the interests of a state rather than a cybercrime gang. A state that was in conflict with Ukraine was using cyber-attacks as a policy achievement tool. As one security analysis explained, the malware also sent a political message that doing business in Ukraine exposes you to cyber-attacks (Kirk, 2017). Western companies with offices in Ukraine like Maersk and FedEx/TNT were given notice to watch out if you continue to do business in Ukraine. We will return to Ukraine later. Next we will focus on the next piece of bad news, which further indicated a darkening landscape for critical infrastructure.

In the summer of 2017 reports of a new weaponized form of malware specifically designed to disable and damage electric power grids were published by antivirus company ESET (ESET/Lipovsky, 2017) and by the industry's Electric Industry Information Sharing and Analysis Center (E-ISAC) (ICS, 2017) a division of the North American Electric Reliability Corporation (NERC, 2018). In short, the new malware called by the names Industroyer/CrashOverride was being described as the 'first operational technology malware designed specifically to attack electric grids' (Butrimas, 2017). The sophistication of the malware demonstrated an advanced knowledge of industrial control systems and high persistence in developing the attack over time. In sum, this malware represented a new kind of cyber threat to industrial control systems used to monitor and control critical processes found in a nation's critical infrastructures. The words 'advanced', 'persistent', and 'threat' in the abbreviation 'APT' is a term commonly understood among cyber security professionals to mean the malicious cyber activities of states. Industroyer/CrashOverride has been named as the cause of the blackout that took place in the capital of Ukraine, Kiev at the end of December 2016. The appearance of this new APT from cyberspace is significant. Lipovsky (2017) claims the Industroyer being the biggest threat to Industrial Control Systems (ICS) since Stuxnet the 'malware was developed to exploit vulnerabilities in those systems and communications protocols they use – systems developed decades ago with almost no security measures'.

In the fall of 2017 I visited Kiev, Ukraine as part of a team that conducted training and table-top exercises in energy security. We had a chance to work with and learn about the energy security landscape of Ukraine from, representatives of government, think tanks, industry, and non-governmental organizations. By 2017 the Ukrainians had experienced several cyber-attacks on their industrial control systems. I noted the decade-long efforts by the Ukrainian utility operators to modernize their Supervisory Control and Data Acquisition (SCADA) equipment with the latest systems manufactured by known Western brands. These cyber-attacks had serious implications. APT groups were using Ukraine as a 'laboratory' to test cyber-attack weapons and techniques on western made control systems. Considering that the operators can only purchase from just a handful of manufacturers of this specialized equipment (just as there are few besides Microsoft that provide PC operating systems) the same form of attack can be applied to other operators of critical infrastructure throughout the world.

Safety Instrumented Systems become a target

The apparent success of state made malware as a relatively cheap, effective and deniable means to a desired end and the lack of international response, attracted significant attention. In December 2017 the US Government, private security companies and security journals

reported about a cyber-attack targeting the control and safety instrumented systems (SIS) of a petrochemical plant located in the Middle East (Kovacs, 2017).

The malware found in the petrochemical plant known as Hatman, Triton or Trisis was a specifically targeted remote access trojan designed to compromise the safety controllers of a triple-redundant safety system manufactured by Schneider Electric (Forney & King, 2017). It was determined that the attack on the control systems of the petrochemical facility was well underway and had progressed to the point of delivering the executable payload to the safety system when something went wrong. It appears the attackers made a mistake in the code and, before executing any attack commands, the safety systems sensed something was wrong and safely shut down the plant. The attackers failed to remove some bugs in their attack software (Perlroth & Krauss, 2018). Tragedy was avoided by the sloppy programming of the attackers and by the plant's staff who, while being unaware of the initial compromise, had the curiosity to investigate why the plant had shut down.

The significance of the Hatman and other attacks on industrial control and safety systems is the focus on compromising and taking over the control of a safety system– a serious escalation of the cyber threat to critical infrastructure. Control and safety systems are used in an industrial process to protect property and, most importantly, people from serious harm resulting from an industrial process that has gone outside of set parameters. These parameters are used to program an automatic response to bring a system back to a safe state when changes in temperature, flow rates, pressure, frequency or other system state indicators exceed pre-set levels.

In other words, SIS are the systems that, for example, automatically shut down a nuclear reactor when something goes wrong with the cooling and pumping systems. If something is done to intentionally neutralize the functions of safety systems, serious harm can result. It is like disabling the breaks and seat belts without the knowledge of the driver while he is driving down a highway. Nothing immediately bad will happen to the driver of the car, but if there was a sudden need to stop the consequences could be tragic. Safety systems are the last line of defense provided by automated technologies to save us from having to deal with something 'going boom in the night'. This emerging danger represents a far different kind of cyber threat than what IT cybersecurity specialists are trained for. It has nothing to do with stealing of data in a document, dealing with a web defacement or a denial-of-service attack. IT events are recoverable with no harm done to the human being or the environment. In most cases rebooting the computer or installing a software update will be bring the IT system back. On the other hand, in a compromise of a control or safety system recovery is counted in terms of costs for replacing damaged equipment, damaged property, injured personnel, and even innocent lives.

Reports and analysis of cyber-attacks on Ukraine's ICS, Hatman, CrashOverride and other incidents affecting industrial control and safety systems have not received their deserved attention or led to any significant changes in policies. One would think that a report of an APT with access to a malware specifically designed to disrupt and damage electric power grids would get serious attention in the industry, however, few are getting the message. I experienced this when I presented a copy of the E-ISAC report on Industroyer to a security official working for a natural gas pipeline. He thanked me for the report but seemed to dismiss it by claiming that natural gas systems differ from electrical ones. I just wanted to make sure I understood him correctly and asked if they were using the SCADA system to which the answer was affirmative. Moreover, to the question of whether they rely upon communications to remotely manage compressor stations and other remote devices, again the answer was affirmative. I attempted to point out that Industroyer can be adapted to attack and disable other industrial control systems.

Now let us take a break from cyber technology and look at the response of the international cybersecurity policy community.

Lack of success in the area of international law and confidence building measures for cyberspace

It can be argued that since 2010 we have witnessed the emergence of a new level of state-associated cyber threats against the critical infrastructure modern economies and societies depend upon for their basic functions. Since states appeared to be involved and considering the fact that critical infrastructures have a cross-border dimension, one would think that the international security community would take notice and respond with appropriate action to manage this dangerous activity. Unfortunately, the efforts made thus far have led to few relevant agreements on confidence-building measures (CBMs) that could support the establishment of a more manageable and stable security environment in cyberspace.

Perhaps the biggest setback at the international security policy level took place during the summer of 2017 during meetings of the United Nations Group of Governmental Experts (GGE). The focus of the GGE, since 2004, has been to study State responsible behaviour in their use of information and communication's technologies (ICT) and of the need to take measures against cyber threats (UNGA, 2003, 2016). The GGE's report for 2015 featured an important recommendation: 'a State should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure' (UNGA, 2015) This was a very welcome concrete step toward promoting responsible state behaviour in cyberspace. Unfortunately, the work seemed to pause for a break in 2017 over disagreements that some commentators saw as politically motivated (Schmitt & Vihul, 2017). The reason for the failure can be explained in two ways. First, the cyber superpowers are behaving like children who resist anyone taking away a favourite toy. Cyber weapons are attractive instruments for policy achievement and/or coercion which are cheap (for a state), effective, and most importantly, deniable. If a state is feeling frustrated at being unable to achieve a foreign policy objective through traditional diplomatic means the use of cyber means can be most tempting. A good example is the use of a cyber weapon to stop the Iranian nuclear enrichment programme in 2010, which unfortunately failed to generate much concern among the international community. The second explanation is that the nature of the cyber threats that can paralyze a nation's economy and well-being of society is not understood as a clear and present danger to all. The predictions of a 'cyber war' or 'cyber Armageddon' have failed to materialize and perhaps have contributed to a sense of policy fatigue. The level of appreciation of the problem of state cyber misbehaviour and recognition of the need to come up with a comprehensive solution so far seems not enough to bring about a consensus among nations. However other fresh analysis and hopeful proposals are in development (Tikk & Kerttunen, 2018).

Still, the warnings, wake-up calls, and poorly thought out international responses continue. One disturbing proposal from an international law expert is getting some attention. It is called the 'duty to hack'. The argument goes that the militaries should be given an option to use a cyber weapon to attack a target instead of using a traditional bomb in order to reduce collateral damage. 'Thus, if a State can achieve the same military objective by bombing a factory or using a cyber-operation to take it off-line temporarily, the Duty to Hack requires that State to pursue the latter course' (Hollis, 2014). The building that houses the operations inside the plant need not be destroyed, only the technical process needs to be stopped, and no long-term damage to property or loss of life needs to be calculated into the decision to

attack. This, indeed, sounds attractive. But when considering through the implications from a technical point of view, the shortfalls of this scheme become apparent.

First, if the target of a cyber operation is the controller for a cooling system of a nuclear power station the consequences are difficult to foresee in advance. If a sub-system or a device of a complex process is targeted and intentionally made to fail the process itself may still continue causing effects that are difficult to predict and control. In addition, the failed device can leave out a key safety element in the chain, which can lead to a sequence of events, which may be hard to control. The risks of causing a nuclear meltdown of the reactor are nearly impossible to calculate, especially, if one considers the consequences of using cyber means to disable a plant's safety instrumented systems. It is likely that the photographs of a nuclear power station after a cyber-attack or a bombing attack are likely to look the same; here we can recall the photographs of the Fukushima nuclear power stations after the earthquake and tsunami had caused the failure of the cooling system in 2011. There is, however, another important difference in employing a cyber weapon instead of a traditional bomb to disable a target that is relevant to this discussion. In the case of a nation's air force dropping a bomb or firing a missile, the country responsible is likely to be identified, while in the case where a cyber weapon is used, the country responsible will likely remain unknown. The accusations without proof by the victim will be weighed against the reasonable doubt produced by the denial of the accused perpetrator. Most specialists agree on who was behind Stuxnet but the suspected perpetrators' silence or public denial is unfortunately enough to introduce enough doubt to limit any appropriate international response.

This lack of attribution capability also affects deterrence as a means to inhibit the use of cyber in an attack or first strike. A potential attacker will be deterred because of fear of retaliation or the lack of success. Cyber capabilities, however, are seen to bring both attractive and destabilizing elements into play when nations come into conflict with one another. Jervis (1978), in his analysis of deterrence posture, referred to a 'doubly dangerous' situation when offense has the advantage and when there is no clear distinction between an 'offensive' and a 'defensive' posture. The capabilities used, and the skills sets created for the conduct of cyber defence or cyber offense operations, are very similar, and capabilities governments often justify as being developed for defensive and intelligence purposes can also be employed for offensive purposes. For this additional reason, the 'duty to hack' proposal is the most destabilizing and dangerous. The advantages of effectiveness, low cost of execution, and deniability provide a significant temptation for a state that is frustrated in failing to achieve a policy objective. Our international lawyers and diplomats of cyberspace policy will fail us if they do not understand the problem's implications from a technical standpoint. The lawyers and diplomats who sit around conference tables discussing norms, rules and principles and CBM's need to add a few chairs for the cybersecurity professionals and engineers to get a full view of the problem.

Another issue that is inhibiting effective action is the belief as an acceptable fact of life that cyber espionage represents a modern continuation of an age-old tradition in state-to-state relations. One mistake is being made again because of a lack of imagination and choosing not to have cybersecurity practitioners and engineers present. Network intelligence is not necessarily similar to traditional intelligence. In cyberspace one can use cyber means to collect intelligence from classified networks but, like the agent James Bond, he can, if he needs to, also become a saboteur and physically destroy things by manipulating control systems. The risk factor for cyber espionage is low compared to the risk the traditional spy takes when physically entering a site. While the traditional cloak-and-dagger operative risks being caught as he jumps over the fence the cyber spy can perform his operations afar in the shadows of cyberspace. The cyber

spy only needs to press the <enter>key to become a cyber saboteur. If a cyber spy penetrates a control system it should not comfort anyone when it is said that the espionage activity was conducted only for intelligence purposes. A cyber spy achieving access should be understood as an alert of a potential effect-causing cyber-attack, resulting in degraded system performance or destructive damage. Another destabilizing factor leading to increased distrust among nations. As Schneier (2014) argues, electronic espionage is not just about overhearing a conversation or passively monitoring a communications circuit but can also become active breaking into an adversary's computer network and installing malicious software designed to take over that network, which is an offensive action violating the sovereignty of another country.

There is one ray of light coming out of the darkness. The private sector is a source of a very promising proposal for a confidence and security building measure. This came from Microsoft Corporation in its proposal for a 'Digital Geneva Convention' (Ciglic, 2018). One of the key proposals echoed what the UN GGE recommended in 2015: 'Government should agree not to attack civilian infrastructures, such as the electrical grid or electoral processes' (Leyden, 2017). It is one of the most perplexing things to consider that proposals like this are so quickly brushed aside. (CCDCOE, 2017) The criticisms range from the dangers of proposing an unwarranted and dangerous questioning of the applicability of established international law to self-serving motives of corporate self-interest (Parker, 2017). It was astonishing to read reactions from some colleagues working in the field of CBM to the Microsoft proposal. For example, one response was that 'they [international security policy makers] believe it would be an extraordinarily bad idea, that any agreement would codify something far worse than the present situation'. Proposals, as well as voluntary norms, for managing the dangerous trends in cyberspace may, when adopted without due consideration, undermine the existing higher standards of international law. Yet, breaking an agreed pledge to restrain from malicious cyber behaviour can at least raise the bar of deterrence.

One can only conclude in considering the continuing and increasingly sophisticated cyber-attacks directed at the control systems that such talk must give great comfort to the perpetrators. It may even encourage them to proceed further since they know they will not be hunted down and prosecuted as in the case with cybercrimes. Even though there is a Cybercrime Convention international law enforcement will not pursue an investigation further if it leads to the activities of a state. To quote the director of one law enforcement agency 'But as soon as we find out that it's state-sponsored, or there may be state actors involved, we back away from that' (Sadauskas, 2015).

Addressing the problem from the engineering side

There is perhaps a good outcome to the Hatman story. It has attracted the attention of industry, manufacturers and the engineers. Soon after the Hatman story broke, two workgroups were created to deal with the problem of cyber vulnerable industrial devices. The International Society for Automation's Committee on Industrial Automation and Control Systems Security (ISA, 1999) created a subgroup (WG4 TG7) to come up with recommendations for dealing with the lack of cybersecurity found in Level 0 and 1 industrial devices of the Purdue Model (Pera, 2018). These are the devices that are closest to the physical process such as actuators, sensors, program logic controllers and safety devices. It is the objective of this group to provide cybersecurity guidance to ensure the safety and reliability of those devices already installed and to guide the secure design of new devices.

A European Union institution took the initiative to create a workgroup to deal in part with the issues raised by Hatman. The Industry 4.0 Cybersecurity Experts Group (EISA)

created in early 2017 by the European Union's ENISA (ENISA, 2017) 'aims at gathering experts at the crossroads of industrial systems and Internet of Things (IoT) to exchange viewpoints and ideas on cyber security threats, challenges and solutions'. As with the ISA group the EISA group also includes representatives from manufactures and policy makers.

While the engineers can do a lot to increase domestic resilience and reduce the possibilities of a cyber-attacks causing major damage to critical infrastructure, they need some help from the international security policy community. The resources that a state can apply to the support of malicious cyber-attacks at another state's critical infrastructure are beyond what the engineers working in isolated power plants and petrochemical facilities can accomplish. They, together with designers of new systems, need some breathing space to catch up to the scale of the threat in order to design safer and more reliable systems. The odds they are up against are quite high. An engineer working on keeping a power grid up and running cannot compete against a state sponsored APT that may already have penetrated his control systems without his knowledge. The outcome of the engineers' defensive effort is as predictable as the outcome of a soccer match between a high school team and a World Cup team.

The question remains: if the engineers need help with defending their critical operation from state resourced APT cyber-attacks and law enforcement does not take up the case then who does? This is the challenge for international law and security policy practitioners.

Some help could be on the way: A modern-day "Fourteen Points" proposal for peace in cyberspace

On January 8, 1918, after the 'war to end all wars', US President Woodrow Wilson made his proposals for a peace treaty at Versailles called 'The Fourteen Points'. Let us see if some of those fourteen proposals can be adapted to promote peace in cyberspace today. Taking into account the original points that are no longer applicable, here are:

Eight points for twenty-first century cyberspace

1. States commit to transparency in regard to their cyber activities
 - One of the desired outcomes would be the re-establishment of trust in cyberspace to prevent unintentional or unmanaged escalation of a new cyber arms race;
2. People's freedom to access and make use of the Internet for the pursuit of knowledge, commerce and happiness
 - Supports a report (UNGA, 2011) to the UN General Assembly which stated that access to the internet is a human right;
3. States agree to restrain from directing malicious cyber activities at the critical infrastructure of other states
 - Supports UNGGE 2015 recommendations and could be the basis for arriving at a common ground: States should agree that it is in their own interest to protect the infrastructure their economies and society's well-being rest upon;
4. States agree to remove all 'logic bombs' or malware placed in the critical infrastructure of other states
 - Useful for controlling rises in tension among states. One can imagine the pressures on targeted Governments to do something when such bombs are discovered;

5. States agree to make every effort to promote trust on the Internet
 - The Internet first came about because of trust between those wishing to connect their systems for mutual benefit. The Internet now risks becoming much less than what it was once promised to be;
6. States agree to take responsibility for malicious cyber activities taking place inside or transiting through their cyberspace jurisdictions
 - Allows for the possibility of applying soft pressure on states who deny responsibility in spite of evidence to the contrary;
7. States agree to respect each other as equal stakeholders in managing and using the Internet and respect the legitimacy of each other's culture as expressed in cyberspace
 - This may be a controversial point as it contends that there are nations which may be seeking either intentionally or because of their de facto pervasive technical presence as dominating or 'colonizing' the Internet;
8. States agree to create a coalition of willing experts and institutions to monitor and advise on violations of the above agreements
 - This point will also address the attribution issue. What has been lacking up to this point is the will among nations to cooperate and share information. Something that is evident in fighting cybercrime but missing from countering malicious state cyber activities in cyberspace.

If these proposals are to be effective, special care must be made to address the issues that caused the failure of the original Fourteen Points. The actions of the aggressors in the 1930s instead of being checked, continued to see the rewards of their bad behaviour toward their neighbours. Perhaps the realization of today's technological interdependence will change this kind of thinking and help open some blocked doors. There are signs that this realization is beginning. In 2011 the German Bundestag issued a study on the effects of a prolonged blackout in Europe (Peterman et. al., 2011). This comprehensive study brings out the cross-sector consequences of a lack of electricity characterizing it as a 'national disaster' where the Government cannot guarantee the security of its citizens. The report concludes 'that even after a few days, it is no longer possible to guarantee area-wide supplies of vital/necessary goods and services to meet the population's requirements within the region affected by the blackout. Public safety and security is jeopardized; the state can no longer meet its duty of protection, as anchored in the Basic Law, to protect the life and limb of its citizens. The state therefore also loses one of its most important resources – the trust of its citizens' (Peterman et al., 2011, p. 232).

Conclusion

Today's state-sponsored threats emanating from cyberspace are increasing in frequency and degree of sophistication. These perpetrators, like terrorists, have also started to exhibit a willingness to disregard the consequences for their actions on the innocent. In the past ten years state-sponsored malware have evolved from specifically targeted and limited attacks, as demonstrated by the Stuxnet operation against a nuclear enrichment facility (Langner, 2013 and 2016), to seeking maximum random damage as demonstrated by the perpetrators of the

NotPetya and potentially by the Hatman attacks discussed earlier. Unlike the coordinated and successful international efforts to confront cybercrime such as the European Council's Convention on Cybercrime the efforts to manage malicious cyber activities of states have been trivial when considering the threat state resourced cyber weapons pose to humanity. The lack of an international security mechanism to manage the risk and discredit the argument that using cyber weapons against another state is effective, cheap and deniable can only contribute to furthering this destabilizing behaviour that risks much wider and more dangerous conflict. This is just the opposite of what is needed at a time when states' and people's fates are far more interconnected and dependent on each other for well-being than ever before.

This chapter has attempted to demonstrate that the stakes in terms of the safety and reliability of our critical infrastructure and threats to them are quite high. An effort is required to reduce the danger and likelihood of damage and loss of life that would come from a major failure occurring in the technologies that today support the modern economic life and well-being of society. References have been made to the First World War, a war that caused terrible suffering to citizens which was accompanied by economic and political shocks that are felt to this day. In hindsight many wonder how those leaders allowed a single political assassination to go so out of control. While it may be stretching the imagination that a nation's cyber-attack on another's critical infrastructure could lead to such a destructive and wide-spread conflict as a world war, it would be worth the combined effort of concerned leaders from governments, industry, and private citizens to learn from the lessons of World War I and ensure that such an event will never take place. We should in future be guided by a desire to finish the job. As Winston Churchill is thought to have said: 'It is no use saying, "We are doing our best." You have got to succeed in doing what is necessary'.

References

- Amir, W. (2016) Hackers claim stealing NSA hacking tools: Selling them online. *HackRead*. Weblog. Available from: www.hackread.com/hackers-claim-stealing-nsa-hacking-tools/ [accessed 16 October 2018].
- Butrimas, V. (2017) Threat intelligence report: Cyberattacks against Ukrainian ICS. *Sentryo*. Available from: www.sentryo.net/wp-content/uploads/2017/09/Ebook_Cyberattacks-Against-Ukrainian-Ics.pdf [accessed 16 October 2018].
- Ciglic, K. (2018) Cybersecurity Policy Framework. A practical guide to the development of national cybersecurity policy. *Microsoft*. Available from: www.microsoft.com/en-us/cybersecurity/content-hub/Cybersecurity-Policy-Framework [accessed 16 October, 2018].
- Cooperative Cyber Defence Centre of Excellence (2017) Geneva Conventions apply to cyberspace: No need for a 'Digital Geneva Convention'. Available from: <https://ccdcoe.org/geneva-conventions-apply-cyberspace-no-need-digital-geneva-convention.html> [accessed 11 August 2018].
- Crozier, R. (2018) Maersk had to reinstall all IT systems after NotPetya infection. *itNews*. Weblog. Available from: www.itnews.com.au/news/maersk-had-to-reinstall-all-it-systems-after-notpetya-infection-481815 [accessed 16 June 2018].
- Electricity Information Sharing and Analysis Center (2017) ICS Defense Use Case No. 6: Modular ICS Malware. *SANS/E-ISAC* Available from: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf [accessed 16 October 2018].
- ESET (2017) Industroyer breakdown: Q&A with ESET Malware Researcher Robert Lipovsky. *ESET*. Available from: www.eset.com/us/about/newsroom/corporate-blog/industroyer-breakdown-qa-with-eset-malware-researcher-robert-lipovsky-1%20June%2020/ [accessed 20 May 2018].
- European Union Agency for Network and Information Security (2017) EICS Experts Group. Available from: <https://resilience.enisa.europa.eu/eics-experts-group> [accessed 20 July 2018].
- Forney, P. & King, A. (2017) TRITON. *Schneider Electric Analysis and Disclosure Conference*. Video presentation. Available from: www.youtube.com/watch?v=f09E75bWvkk&feature=youtu.be [accessed 20 September 2018].

- Gilbert, D. (2015) Equation Group: Meet the NSA ‘gods of cyber espionage’. *International Business Times*. Available from: www.ibtimes.co.uk/equation-group-meet-nsa-gods-cyber-espionage-1488327 [accessed 16 October 2018].
- Goodin, D. (2017) An NSA-derived ransomware worm is shutting down computers worldwide. *arsTechnica*. Weblog. Available from: <https://arstechnica.com/information-technology/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/> [accessed 16 October 2018].
- Greenberg, A. (2018) The untold story of NotPetya, the most devastating cyberattack in history. *Wired*. Available from: www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [accessed 16 September 2018].
- Hollis, D.B. (2014) Re-thinking the boundaries of law in cyberspace: A duty to hack? *Temple University Legal Studies Research Paper No. 2014–16*. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2424230 [accessed 16 June 2018].
- Jervis, R. (1978) Cooperation under the security dilemma. *World Politics*. 30(2): 167–214. Available from: www.jstor.org/stable/2009958 [accessed 18 June 2018].
- Kirk, J. (2017) Latest ransomware wave never intended to make money. *Bank Info Security*. Weblog. Available from: www.bankinfosecurity.com/latest-ransomware-wave-never-intended-to-make-money-a-10069 [accessed 16 October 2018].
- Kovacs, E. (2017) New Triton ICS malware used in critical infrastructure attack. *SecurityWeek*. Weblog. Available from: www.securityweek.com/new-ics-malware-triton-used-critical-infrastructure-attack [accessed 10 October 2018].
- Langner, R. (2013) To kill a centrifuge: A technical analysis of what Stuxnet’s creators tried to achieve. *Langner Group*. Available from: www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf [accessed 7 October 2018].
- Langner, R. (2016) Stuxnet attack code. Deep dive. *Langner S4*. Video presentation. Available from: www.youtube.com/watch?v=zBjmm48zwQU [accessed 7 October 2018].
- Leyden, J. (2017) Microsoft president says the world needs a digital Geneva Convention. *The Register*. Available from: www.theregister.co.uk/2017/11/10/microsoft_president_calls_for_digital_geneva_convention [accessed 15 October 2018].
- Parker, B. (2017) Bots and bombs: Does cyberspace need a ‘Digital Geneva Convention’? *Irinnews*. Available from: www.irinnews.org/analysis/2017/11/15/bots-and-bombs-does-cyberspace-need-digital-geneva-convention [accessed 16 October 2018].
- Perlroth, N. & Krauss, C. (2018) A cyberattack in Saudi Arabia had a deadly goal. Experts fear another try. *The New York Times* (15 March).
- Petermann, T, Bradke, H., Lüllmann, A., Poetzsch, M., & Riehm, U. (2011) What happens during a blackout: Consequences of a prolonged and wide-ranging power outage. *Office of Technology Assessment at the German Bundestag*. Available from: www.tab-beim-bundestag.de/en/pdf/publications/books/petermann-etal-2011-141.pdf [accessed 7 September 2018].
- Purdue Reference Model for CIM. Available from: www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.html [accessed 16 September 2018].
- Sadauskas, A. (2015) Inside Interpol’s digital crime centre. *itnews*. Available from: www.itnews.com.au/news/inside-interpols-digital-crime-centre-410768?eid=3&edate=20151021&utm_source=20151021_PM&utm_medium=newsletter&utm_campaign=daily_newsletter [accessed 26 July 2018].
- Schneier, B. (2014) There’s no real difference between online espionage and online attack. *Schneier on Security*. Weblog. Available from: www.schneier.com/essays/archives/2014/03/theres_no_real_diffe.html [accessed 16 October 2018].
- Schwartz, M. (2017) Ukraine power supplier hit by Wannacry lookalike. *Bank Info Security*. Weblog. Available from: www.bankinfosecurity.com/ukraine-power-supplier-hit-by-wannacry-lookalike-a-10071 [accessed 16 October 2018].
- Schmitt, M. & Vihul, L. (2017) International cyber law politicized: The UN GGEs failure to advance cyber norms. *Just Security*. Weblog. Available from: www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ [accessed 16 August 2018].
- Suiche, M. (2017) WannaCry – The largest ransom-ware infection in history. *Medium*. Weblog. Available from: <https://blog.comae.io/wannacry-the-largest-ransom-ware-infection-in-history-f37da8e30a58> [accessed 16 October 2018].
- Tikk, E. & Kerttunen, M. (2018) Parabasis. Cyber diplomacy in stalemate. *Norwegian Institute of International Affairs*. Available from: www.nupi.no/Publikasjoner [accessed 16 November, 2018].

- United Nations General Assembly (2003) Developments in the field of information and telecommunications in the context of international security. A/RES/58/32 (18 December).
- United Nations General Assembly (2011) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/17/27 (16 May).
- United Nations General Assembly (2015) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174 (22 July).
- United Nations General Assembly (2015) Developments in the field of information and telecommunications in the context of international security. A/RES/70/237 (30 December).
- Weiss, J. (2017) Ransomware and control system cybersecurity. *ControlGlobal*. Weblog. Available from: www.controlglobal.com/blogs/unfettered/ransomware-and-control-system-cyber-security/ [accessed 6 July 2018].

10

STEPS TO AN ECOLOGY OF CYBERSPACE AS A CONTESTED DOMAIN

Martin C. Libicki

Even brief ways of modelling the ebb and flow of combat in cyberspace are useful. Modelling, and thereby understanding implications of actions and counteractions, promotes individual and collective learning and supports the formulation of corporate, governmental, and international policies, even norms of responsible state behaviour in cyberspace. Modelling also reminds us of the risks involved and caution needed when taking offensive action or responses.

A useful model is one that is not necessarily one that gives the right predictions but one induces questions which go to the heart of what is important. By way of example, consider Lanchester's laws – based on the observation that, in a contest of arms in which firepower is the key variable, the strength of a military force is proportional to the square of its size; that is, essentially, a matter of more firepower concentrated on fewer enemy targets. The usefulness of that insight is that it raised the focus on how to distribute forces. For classic naval forces the debate was over whether to concentrate them to win the big battle (à la Mahan) or distribute them in order to raise the peril to merchant shipping (à la the *jeune école* school). Such laws were less an insight about how to operate militaries, and more of an insight into the core trade-offs that militaries face when making operational decisions.

In cyberspace, mass does not matter so much; indeed, it is unclear how to define it at all. Instead, we will argue that the co-evolution over time between offence and defence may assume comparable importance – although it may not yield an expression as pithy as Lanchester's laws provided.

Scope and caveats

The co-evolution of offence and defence takes place globally, largely because knowledge about cyberspace, in much the same sense that mathematics is, is global. This dynamic takes place through cyberespionage as well as cyberattack; against civilian targets and military ones; in today's peacetime environment, and, in all likelihood, in a wartime environment. Nevertheless, it may help to think of the contest as involving a strategic warfare campaign – one in which the attacker is primarily attempting to impose costs on the defender. The defender seeks to minimize costs of the cost of bearing cyberattacks *plus* the cost of cybersecurity, itself. Any one state can employ both attackers and defenders.

This contest is played in civilian *and* military domains, but the latter is not necessarily characteristic of the whole. First, it is unclear that a purely cyberspace campaign against deployed military forces are efficacious in military terms – although it could be (Gasperre, 2008; Crowdstrike, 2016). By contrast, in understanding cyberspace operations at the strategic level, we know that hackers have imposed serious costs on civilian enterprises with the NotPetya worm being the most prominent example. Second, military campaigns tend to be episodic and, among cyber-sophisticated adversaries, episodes can be short and intense – whereas a full appreciation of the dynamics of cyberspace needs to span time to consider action and reaction. Third, particularly for military targets, carrying out cyberattacks can jeopardize accesses used for long-term cyber-espionage and may thus be the rarity rather than a norm. This trade-off is far more muted when going after critical infrastructures such as power grids.

Focusing on cyberattack as prototypical rather than the more frequent cases of cyberespionage, gives scope to assess what an unrestricted cyberattack campaign would look like. Furthermore, while cyberespionage is meant to steal information noiselessly, the effects of cyberattack are often unmistakable. This makes cyberattack easier to spot after the fact – even if it is going too far to assert that all cyberattacks are discovered and characterized as such, while no acts of cyberespionage are. But when cyberespionage is detected and its effects are deemed consequential, they can spur defences in ways similar to what cyberattacks can. As for cybercrime, there are so many different attackers that, with a few possible exceptions (Trend Micro, 2018), the decisions of any single attacker have minor consequences for what defenders do. Finally, we ignore distributed denial-of-service (DDOS) attacks as they are of limited utility and generally arise from factors outside the defenders' direct control.

This treatment lacks equations and thus numbers. When relationships among variables are simple, words tend to communicate more easily. As the relationships get more complicated or the number of factors increase the difficulty of communicating what is going on rises exponentially; at that point mathematics helps communicate. But the valid use of equations requires high degrees of specificity and measurability. Specificity, alas, is a problem: a belief that some defenders are better than others can be expressed for example parametrically (e.g., '1' if well-prepared, '0' otherwise) as a point on a 0–1 line, as a standard distribution (e.g., the Bell curve), or as a power-law distribution. Measurability is a worse problem: when it comes to cyberspace incidents N is small, examples are highly variegated and thus difficult to characterize, attackers do not identify themselves much less fill out detailed questionnaires, and defenders are almost as tight-lipped and are anyway not always sure exactly what happened at the point where they have to react. At the high end, cyberspace intrusions are often one-offs, almost by definition, and any domain characterized by coupling between measures and countermeasures inevitably evolves too fast to be the subject of formal modelling. Instead, it is toward a heuristic model that we build.

We proceed by stating seven propositions which should supply the foundation for understanding the dynamic ecology of conflict in cyberspace – and the possible implications on international peace and security, including stability.

Proposition: Because there is no forced entry in cyberspace measures beget countermeasures

Hackers generally breach systems by finding paths that already exist through a combination of stolen credentials and software vulnerabilities.

One big difference between exploiting software vulnerabilities and stealing credentials is that software vulnerabilities can be fixed once and for all while credentials hijacking,

which depend on the vigilance of the victim, is not as amenable to a once-and-for-all-time fix. Such differences, though, are often a matter of degree rather than kind. First, exploits and credentials hijacking often facilitate one another. Second, while a patched vulnerability may seem like a now-and-forever fix, patches do not circulate everywhere instantly, and new vulnerabilities emerge even, perhaps especially, from existing *vice* new software. The history of Eternal Blue exploits merits note in that while its original developers discovered the vulnerability before writing their exploitation, those who used it later, notably the attributed authors of WannaCry (North Korean Lazarus group) and NotPetya (Russian military intelligence agency, GRU), did so after the patch was issued. Third, there are some once-and-for-all-time approaches to credentials safekeeping, such as multi-factor authentication, or fixing server-side vulnerabilities that permit stealing credentials wholesale.

More broadly, architectural features of a network – essentially, what people and processes can read from or write to whom about what – also predispose systems to greater or lesser levels of cybersecurity. Changing the architecture is an option (actually a set of many options) that defenders can take to limit the damage or accelerated the recovery from cyberattacks. Some such changes, such as revoking certain privileges or isolating sub-networks, can be undertaken quickly; others can take months and years of work. Between 2001 and 2004, for instance, the Internet was buffeted by a succession of worms (e.g., Code Red, and Slammer) that fed on Microsoft operating systems. Each worm was quickly patched – but they kept coming because there were some fundamental design problems with these operating systems, notably, its Internet Information Services. Only with the issuance of Microsoft Windows XP Service Pack 2 in August, 2004, that is, three years after Code Red emerged, were such issues effectively put to bed.

***Proposition: The offence-defence dynamic vies with the
state-on-state dynamic***

In almost every other military domain, a dyadic contest can be characterized as one military entity versus another. Operational adaptation and, to a great extent, technological change is driven by such competition. Historically, this competition has had elements of symmetry or force-on-force: one side's infantry versus another's or one side's capital ships versus another's.

More recently, there has been a rise in the importance of two-sided competition, notably between hiders and finders – think stealth aircraft v. radar, submarines v. anti-submarine warfare, and ballistic missile defences v. long-range missiles. This fact often entails setting up two simultaneous competitions: e.g., one side's detection techniques versus the other side's submarines and one side's submarines versus the other side's detection techniques – but with some convergence such as when two submarines are hunting one another.

The competition in cyberspace has many such characteristics; in other words, one side's defences contend with their offences and vice versa. But the *broader* competition between offence and defence is determined largely *outside* of dyadic military competition. The state of this broader competition can be proxied by the amount of effort attackers must employ to subvert a targeted system – and how much effort defenders must employ to limit their damage down to acceptable levels. It is *not* a matter of whether offence or defence is dominant, a question of limited meaningfulness, anyway.

Thus, the competition in cyberspace differs from almost all other military competitions. Granted, many military systems borrow features from civilian systems and vice versa.

Military competition drove aircraft design in both World Wars and civilian advances in aircraft in the interwar period were incorporated into military designs. But when the armed forces concluded that their aircraft needed stealth, there was no civilian counterpart to such advances. Buyers of civilian aircraft do not worry overly much about the competition from surface-to-air missiles – actually, calls to harden commercial aircraft against terrorist-wielded weapons have never been answered. Similarly, maritime cargo operators do not worry about engineering acoustic quieting, nor are civilian trucks designed to spoof overhead aircraft. In cyberspace, however, most of the techniques used to protect military systems are available for civilian systems – and almost all of the techniques used to protect civilian systems are available for military systems.

In other words, the dominant dynamic of most military competition arises in the military world – but the dominant dynamic of competition in cyberspace arises in the civilian world: mostly in defence, and, even, to a large extent in offence.

The offence–defence competition in cyberspace would be similar, but less intense, in a world without national security competition. Corporations, for instance, would have to defend their networks against criminals and malicious insiders – who use many of the same techniques used by state-sponsored hackers. Nevertheless, state-sponsored attackers tend to accelerate the pace of measure and countermeasure; they are more likely to use zero-days than criminals are and are somewhat more likely to strive for persistence. Criminals, on the other hand, are more likely to go for a payoff and then leave, but in some cases, some persistence may be required to get to that payoff. On the defence side, state intelligence agencies develop cryptographic technologies, can provide key customers with insights about specific attackers, help populate national-level firewalls with signatures, and contend with adversarial hackers within networks to frustrate their evil designs.

So, the contest in cyberspace has two near-orthogonal vectors: offence versus defence, and state versus state. Of the two, the offence–defence contest is primary because it establishes what can and cannot be done in cyberspace. Were there a broad theory about the contest for cyberspace, akin to these Lanchester equations, it would largely be about offence–defence interactions – they determine the terrain of battle. National capabilities – both offence but also defence and the dependence of national security on the contest in cyberspace – manoeuvre, so to speak, upon that terrain.

It is only a small exaggeration to argue that defence efforts are global while offensive efforts are national. Nearly all individuals, academics, organizations, and civilian government agencies prefer there be more cybersecurity. Except to protect some investigative techniques, the law enforcement, intelligence, and military communities promote cybersecurity. White hat, corporate, and government cybersecurity experts cooperate both in the specific and in general to build a science of cybersecurity. National computer emergency response teams (CERT) even from competing countries, such as China, South Korea, and Japan, exchange data with one another, and cybersecurity firms have global clients lists. Vendor patches are available worldwide; they make all of their clients more secure.

By contrast, cooperation at the offence level is far less developed. With the notable exception of the Five Eyes (Australia, Canada, New Zealand, the United Kingdom, and the United States) cooperation, rarely do state intelligence agencies, the predominant source of offensive expertise, cooperate with one another. The best example of attacker cooperation arises in cybercrime markets – as well as the trade among cybercriminals and some state-sponsored hackers. And the same lessons about what works and fails are available to them as well as to defenders.

Proposition: Cybersecurity is carried out at two levels: by defenders and by vendors

The cybersecurity terrain, we now argue, can be understood in terms of two broad classes of effort: those undertaken by organizations *qua* network owners, and those undertaken by software vendors, including the open source community, and vendors of hardware with software-defined features. By contrast, a successful hack will involve failures on the part of both.

Vendors fail by having software with vulnerabilities. Even if vulnerabilities are patched at the time of entry – which may precede cyberattack or data exfiltration by months or years – patch installation and testing is not always easy. As noted, the Eternal Blue exploit's most disruptive use was *after* its patch came out. The 2017 Equifax hack exploited an open source vulnerability for which new clean code had been available. Vulnerabilities are but one aspect of software failure. Others include the software's architecture – such as whether browsers run in a sandbox (e.g., Chrome versus Firefox circa 2014 (Gooden, 2017)), or the protections available against the attachment of rogue code (e.g., iOS versus Windows) to the operating system. Also important is how well the user interface facilitates the intelligent selection of, say, a computer's security settings or a social network's privacy settings. Finally, recent software supply attacks teach that vendors need to ensure that the code they write is the code they ship; many notable hacks succeeded by subverting the code in the factory, so to speak.

The community of packaged-software vendors is concentrated. Microsoft has a far greater influence on the course of cyberwar than any one network owner – the US Department of Defense excepted. Conversely, few vendors of cybersecurity products and services are also large. But smaller vendors sometimes matter; a supply chain attack on the vendor of MeDoc, who makes accounting software for Ukrainian taxes, enabled NotPetya. Furthermore, the burgeoning Internet of Things (IoT) will introduce many small *hardware* vendors into the cybersecurity environment who have little experience in writing software or, worse, maintaining it after it is sold (Schneier, 2017). Conversely, the larger vendors may be able to cover faults introduced by smaller vendors: examples include how Google's Chrome treats extensions, how iOS limits what iPhone apps can do, or the potential melioration that home routers or controllers can provide against errant home IoT devices.

Network owners are generally responsible for the rest of the cybersecurity environment. They buy the software and can, in theory, if not so easily in practice, reject insecure software in favour of secure software, or at least sometimes set security levels in such software. More importantly, they control which employees and business partners can access what parts of their systems, how networks are connected to one another, what cybersecurity products and services are used, the level of organizational resilience and the speed and completeness of its recovery after an attack. The quality of an organization's cybersecurity posture is a function of the understanding, diligence, and budget of its systems administrators – but improvements in network management tools, such as those that detect differences between network policies and network practice, can improve cybersecurity even given the quality of systems administration.

The example of Stuxnet shows both vendors and network owners creating the environment that predispose attackers to fail, or, in this case, succeed. The example also manifests how technical and organizational cybersecurity issues can be intertwined with those of national and international security. Starting with vendors, Microsoft's Windows operating system at that time had four zero-day vulnerabilities, and Siemens, who made the programmable logic controller, used a hard-wired, and widely known, password to 'protect' its

devices. But the attack's success was also fostered by mistakes made by those managing the Natanz uranium enrichment facility: allowing a USB device into the facility, using the same device to control *and* monitor the centrifuge network, neglecting to install hardware-based safety features, and being inattentive to audible anomalies in centrifuge rotational speeds.

When it comes to countermeasures, vendors are likely to respond in different and more systematic ways to having suffered from offensive cyberspace operations than network operators will. Vendors are likely to be more sophisticated. They can also be held responsible by customers for the cybersecurity weaknesses in their offerings: for cybersecurity products, and increasingly, cloud providers, it can *potentially* be the great differentiator among rival firms. By contrast, organizations are less likely to be held responsible for the quality of their cybersecurity, except by their own customers but only in those cases where customers are affected by such cybersecurity shortfalls, for example, because their privacy has been violated. The Equifax hack illustrates shortfalls in this process – although hundreds of millions of individuals had their data exposed to the hackers, these individuals were not ‘customers’ of Equifax; having no say in whether Equifax carried information on them, they could not hold such organizations accountable.

Although vendors vary in their diligence and their reactions to cyberspace incidents, they experience similar pressures to improve their performance. The pressures put on organizations, however, vary greatly. One difference between vendors and organizations is that the latter may be bifurcating in terms of their hardness to cyberspace operations. There are those that are quite committed and responsive to bad events; they tend to include militaries, banks, and Internet service providers, many of whom sell cybersecurity services. The rest include individuals, small businesses, civilian government, and large businesses whose expenditures and responsiveness lag the threat. Fortunately, the critical targets tend to be hardened while the vast mass of noncritical targets are not. Unfortunately, there are exceptions; obscure organizations that occupy disproportionately critical niches in an economy may be grounds for concern.

Putatively, the distinction between diligent and indolent organizations colours how hackers may approach them: either by looking or buying vulnerabilities and designing exploits around them or by reverse-engineering patches to discover which vulnerability has been fixed and then develop exploits for such vulnerabilities. The vulnerabilities-first model differentiates weakly between strong defenders – with multiple layers of defence throughout their system – and weak defenders. The patch-first model differentiates strongly between the patching diligent and the indolent defenders who often have left their systems unpatched. In terms of a strategic cyberattack campaign that could threaten international peace and security, a model that focuses on critical sectors would tend to go up against strong defenders and thus seek zero-day vulnerabilities to pry their way in (or through, after being in). A model that maximizes damage without respect to criticality may succeed by focusing on indolent defenders and can wreak damage by exploiting so-called one-day vulnerabilities, i.e., those just patched.

***Proposition: The measure-countermeasure contest
fosters negative feedback loops***

The relationship of measure to countermeasure suggests that negative feedback plays a large role in the ecology of cyberspace. By way of illustration, consider another domain characterized by negative feedback loops. A perturbation in a system, say a scarcity of a product, creates both demand and supply shifts. If, for example, the price of fuel rises, people drive less frequently, and buy cars which use less gas over their lifetimes: demand goes down.

Simultaneously, the supply (of oil) may increase. A new equilibrium price is reached. Over time, that equilibrium reverts towards its long-run trend, largely because the elasticity of both demand and supply as a function of price tends to rise over time.

In cyberspace, a perturbation of the system, such as a spectacular cyberattack that surprises others because of its method or target, shifts expectations of what cyberspace operations can do, and, unlikely though it may be, perhaps even the balance of power among rivals. But, after the initial shock, people and states adjust. The particular vulnerabilities that allowed such an attack are worked on. The incentives for new cybersecurity tools and policies rise. The general tenor of cyberspace preparedness that allowed a software vulnerability to wreak grows tighter. Follow-on attacks of the same specific type, those that depend on the same vulnerability, fare more poorly, and follow-on attacks of the general type, those that go after a particular class of systems, with time, do not fare so well, either. A new equilibrium is established. Dire predictions that this (cyberattack) changes everything prove unfounded. Granted, the new equilibrium may not equal the old one. Countermeasures can be costly – and if cybersecurity budgets are fixed and manpower is limited, something else will suffer. Implementation is not always complete, and rarely universal. If the cyberattack, in and of itself, creates permanent changes, e.g. in terms of data being destroyed, faith in the assurance of information being sundered, or privacy being violated, such changes do not reverse themselves automatically as the equilibrium evolves. Nevertheless, resilience-building countermeasures do limit the potential of the offensive measures, particularly over time.

Some attack measures are more resistant to countermeasures than others. Professional cyberespionage organizations often work by staring at an organization's network long enough to detect transient lapses that give them entrée (Joyce, 2016). For example, if network administrators address a problem with an expired random-number token-generator by temporarily issuing a fixed token number then evidence of successful reuse may create the opportunity for an attacker to try the same number to hijack credentials. The fixes for such mistakes might be greater organizational discipline and constant monitoring for lapses, but these are not once-and-for-all-solutions.

The contest between measure and countermeasure typifies many contests in conventional warfare, at least as far back as when forts and castles first favoured defenders, who responded with cannon, whose efforts were vitiated by innovations such as the *trace Italienne*, the bastion fort. Nolan (2017) argues that battle appears alluring in the interval between when the offence discovers a novel way of war and when the other side duplicates it or discovers countermeasures. More immediate negative feedback effects are also present; for instance, the further an army advances from its base the more difficult become logistics and communications – both become easier for the side pushed towards its base, a feature Clausewitz saw favouring strategic defence. In other words, negative feedback relationships are important in warfare. But warfare also has *positive* feedback effects, notably whenever a defeat fosters panic which then turns into a rout. Longer run historic dynamics included the process by which conquest yielded people and territory, which, in turn, contributed to the power of the winning military.

Although there are *positive* feedback loops in cyberspace operations, they are both limited and, for the most part, well-characterized. One well-known example is how malware goes viral. Something gets infected, and that infection, in turn, makes it easier for other systems to be infected. This was a problem with viruses in the 1990s, and with worms between 2001 and 2004, as noted. Since then, while there have been system-wide compromises result from spreading infections within organization networks, infections that have spread across the Internet from one network to another have been rare. Another positive feedback mechanism

may arise when intrusions into an organization's network reveal information about other systems so as to facilitate cracking the latter. Again, this mechanism may work within a network but rarely across them.

***Proposition: Time (not space) is the critical feature
of the measure-countermeasure contest***

Time, in this case, is measured in days, weeks, months, and, in the case of a major system rewrite, campaign planning, or national policy re-formulation, years – but not nanoseconds. The tenet that cyberspace operations take place at the speed of light is technically true, but practically meaningless – what it illustrates is not the importance of very short amounts of time but the irrelevance of distance.

An example of a contest in time comes from cyberespionage. An intruder, having succeeded in penetrating the perimeter, wants to use that foothold to move laterally, and, in the process, discover useful information or credentials. The faster the defender finds the intrusion – perhaps because one or another lateral move is anomalous or trigger rarely seen features of the system – the quicker it can determine the signatures and purpose of the intrusion, the better to shield sensitive resources while simultaneously, for instance, eradicating malware and establishing new credentials. For both attacker and defender discovery is a key part of the process. The attacker must discover the target network's architecture and weak points – that takes time. The defender must discover the intrusion and evidence of its traces – that also takes time. Other time-sensitive tasks include, for the attacker, waiting until the defender has let its guard down, and, for the defender, making the correct inferences about the attacker's goals and methods. None of this takes place at the speed for light – but at the speed of human understanding.

Although countermeasures can be developed from research in the absence of discovered measures there is nothing like discovery to accelerate their development and uptake. This is true technically if, for instance, the measure is discovered in post-incident forensic analysis and a countermeasure becomes critical. It is also true psychologically, because reports of great loss, especially if your loss, intensifies search strategies. In many ways, a cyberattack is more likely to accelerate the measure-countermeasure cycle than cyberespionage because the latter is often undiscovered and when discovered, several months have passed after the intrusions began. Nevertheless, if the incentive to change reflects the cost imposed by the attacker, sometimes cyberespionage can impose the larger cost. That noted, the lag between intrusion by an advanced persistent threat and the discovery that cyberespionage has taken place appears to have dropped in the last several years from roughly eight months to perhaps half that today. (FireEye, 2015 and 2017) So, the measure-countermeasure cycle is probably getting faster as well.

Were countries to punish other countries for their intrusions – which the United States does, albeit so far half-heartedly by naming, shaming, and indictments, but no one else seems to – a similar dynamic may arise in which hackers adopt measures to obfuscate their national origins and defenders develop countermeasures that can see through such deceptions. Although criminals subject to apprehension, as many claim in Russia are not, are motivated to hide their identity in cyberspace to avoid jail, their measure-countermeasure cycle for cybercrime is underdeveloped. Knowing where a criminal comes from is only a small step in making an identification, criminals lack many of the resources that states have, and it is the act of monetizing stolen information, something state organizations and hackers rarely do, that often gives them away.

Proposition: Negative feedback loops complicate achieving scale in cyberattacks

The potential for countermeasures, particularly those that can be implemented quickly (e.g., restrictions on access) suggests that scale can be a big problem in extrapolating from successful one-off attacks to a successful campaign, particularly against a large heterogeneous country. This also applies to cyberespionage but with less force and more exceptions.

To illustrate why, imagine an alternative universe in which a system can be taken down by shooting it an exquisitely malformed packet. Those who discover a sufficiently common vulnerability can take down a large percentage of all systems at once through a single shot, albeit widely duplicated. The possibility of scale is inherent in the existence of a vulnerability.

Fortunately for defenders, while hacking systems can work that way (Franceschi-Bicchierai & Cox, 2018), they almost never do. Rather, system subversion is a time-consuming process, in large part because systems are multi-layered and different from one another, not only in construction, but in use and the details of how they are secured. Over the time it takes to amass the basis for a large attack, discovery poses a constant threat to success, particularly when discovery leads to an attack's roll-back before achieving critical mass.

This can be illustrated for attacks that, in order to succeed, must scale vertically, that is, in depth or severity, or horizontally, that is, in breadth (Libicki, 2016).

Start with depth. Many models of hacking presume or state that an attacker must go through several steps to succeed. The 'kill-chain' model posits six such steps: reconnaissance, weaponization, delivery, exploitation, installation, and command-and-control. (Hutchins, Cloppert & Amin, 2010) The Gordon-Loeb model, (Gordon & Loeb, 2002) developed to estimate optimal spending for cybersecurity, posits a more general set of gates that hackers must pass to succeed. What makes such a dynamic interesting is not only the possibility of failure at each step, which characterizes all but the simplest of tasks, but also the likelihood that failure can be detected by the *and* that the attackers can be ejected, and that the target can prevent attackers from using the same paths for re-entry. Given some indication of what to look for, they can find their tracks and remove back doors established by the hacker, remove the malware inserted by the hacker, and void the credentials possessed by the hacker.

Detection may take place because attack activity creates anomalies in the system which, in turn, spur diagnostic and forensic activities, but it can also take place in the interval between steps. The defender, for instance, may be given new signatures to look for; a software patch may point to a newly discovered vulnerability which then induces a review of log files to see if anything had earlier exploited that vulnerability; new cybersecurity software may detect anomalies that old ones missed, and new people may draw inferences from system behaviour that did not hitherto raise concern.

Partial successes by hackers may be more effective than failures at generating defenders' responses. A hacker who sought to take down electric power in a region by attacking the distribution and transmission grid may succeed only in knocking out a neighbourhood. But that event is likely to be noticed nationally, even globally among security communities. There are likely to be attempts to plug specific vulnerabilities – but such news should also raise the general tenor of awareness that electric power installations need greater protection. Short run mitigations may include various forms of isolation and access controls; long-run mitigations may include sophisticated cybersecurity software. The closer attackers get toward a real success the higher the degree of concern – but also the fewer steps these or other hackers need to make in order to claim complete success. Thus, the greater the alarm at lower levels of failure, the better the odds that defenders everywhere have of resisting future

attacks – with the usual caveat against the over-reaction false alarms or the inability to distinguish the everyday run of hacking events from those that indicate real breaches or failures.

In fairness, some attack techniques succeed quite frequently – e.g., phishing, where the point is to get just one person in a large organization to open a corrupted document or access a malign web site; only slightly less successful are attempts to get someone to pass their log-in credentials to a phony log-in page. A direct assault on these problems – such as user awareness and training – will not overcome the laws of large numbers and thus organizational reactions that stress such elements may have minimal effects on cybersecurity. Fortunately, there are indirect remedies – such as code-signing for new or updated software, and multi-factor authentication – which can and do provide considerable resistance.

Similar dynamics govern broad attacks – that is, cyberattacks that require many to be infected to have the impact or influence that hackers or their patrons seek. Again, if enough systems could all be penetrated at once and malware inserted rapidly thereafter then defenders – and more broadly, the cybersecurity community – will have little time to counter such an attack. But attackers looking for a critical mass before lighting off the malware may have to carry out several rounds of penetration attempts – e.g., repeated phishing attacks using different appeals, several subverted web sites to support drive-by infections, the steady but slow growth in the user base of a particular corrupted mobile phone app. The longer it takes to create a critical mass, the more time defenders have to understand the existence, purpose, and signs of malware, and the likelier they are to develop an eradication campaign. The latter could be as simple as a wave of unavoidable patches, or as complicated as rewriting and redistributing open source code libraries. Although large masses of corrupted systems *have* been built over time, for example the Conficker worm (Bowden, 2011) and VPNFilter (Greenberg, 2018), especially to support DDOS attacks, infecting a large percentage of a nation's computers, is more challenging. Time also creates other risks for attackers – a patch or complete software upgrade distributed for other reasons can disable malware incidentally.

Time also gives defenders a way to shake out those classes of attacks wired to go off if certain conditions exist. Something of the sort may be required for cyberattacks against targets which lack a real-time connection to the outside world – such as many military systems, especially in combat. The more time is spent exercising or simulating conditions that would trigger the malware, the greater the odds of detecting such faults in time.

Proposition: Attackers may face dilemmas if they force matters

If time is the enemy of success, then attackers could accelerate the process by which they penetrate systems. But doing so may lead to more failed attempts, some of which may be obvious for lack of painstaking care to hide the attacker's tracks or because the hacker has tried to force opportunities by getting the target system to respond to various sallies rather than wait for such opportunities to arise by themselves through, for instance, temporary weaknesses in systems administration. This could be a problem in accelerating lateral movement within a target system. Similarly, attackers may try several parallel efforts to recruit more systems faster, but the intensity of effort may, itself, trigger suspicions. Many of the efforts to accelerate progress may come at the expense of operational security, failures in which facilitate attribution and characterization.

Attackers could also use several simultaneous tools so that the loss of one of them to discovery does not necessarily end their efforts. But doing this is not free. First, tools are not cheap to generate and master; often, by the point it is obvious that the first tool is reaching its limits, the time available to build the second tool is too limited. But there are exceptions.

Symantec, for example, observed that the Chinese Advanced Persistent Threat (APT), the Elderwood Group, had a stockpile of exploits that allowed them to use another when one was revealed and countered. (O’Gorman & McDonald, 2012) Conversely, unless completely different people are used to make different tools, these different tools will have a familial resemblance; discovering and understanding one tool may give defenders a leg up in finding its cousin. Even if the tools brought forth to work the problem of penetration at one level are very different, the integration between such tools and those used for prior operations (e.g., gaining entry) or for later operations (e.g., triggering unwanted effects) could be squeaky in the sense of prone to failure or detection.

Other dilemmas are associated with targeting. Attackers could launch their attacks at an earlier stage in their development – but at a cost of having weaker attacks. Alternatively, they could go after targets that are softer in the sense of less likely to detect unwanted activity – but, again, at the cost of having less impact.

To be fair, the exact trade-offs involved are matters of speculation in part because examples are few and attackers tend not to publish their thoughts in the open press – but also because the search for tools and techniques that fool defenders as well as those, albeit fewer, that fool attackers is an activity that is inherently difficult to systematize. More insight into the nature of these dilemmas as well as identifying feasible trade-offs are needed.

***Proposition: Faster and wider learning colour
the measure-countermeasure contest***

As a rule, therefore, defences will be better if defenders can learn faster and more efficiently and thereby get ahead of a deepening or spreading cyberattack. Because learning is a useful attribute in all sorts of dynamic environments, the factors that contribute to faster learning are familiar: in particular, a high level of alertness, a systems model or paradigm against which unexpected activity can be evaluated, a willingness to believe that one’s knowledge is incomplete and possibly wrong, and therefore a global culture of cybersecurity in which people, organizations and states are willing to reassess what they know. Conversely, attackers can employ strategies that can suppress the learning that helps mount a reaction to further cyberspace intrusion (Libicki, 2017).

Collective learning has signal advantages over individual learning. If a well-resourced organization develops a set of tools, techniques, and policies that are unique to its given target, the work of detecting and responding to cyberspace intrusions will be limited to the immediate defenders, and advisers, themselves. Knowledge of other tools will be of limited direct help, and what defenders fill will have little applicability to others. But this is quite expensive, hence more an exception than a rule. More typically, tools are recycled or used on multiple targets. Conversely, but similarly, flaws in the architecture or management of systems that permit such tools to work are shared by other organizations.

Everyone speaks fondly of information sharing, especially by others. Unfortunately, the current discourse, as reified in the 2015 US Cybersecurity Information Act has a very constrained view of what information so merits sharing that doing so should be incentivized. Such information is the discrete signatures of known bad actors. It is, however, unclear whether or under what circumstances this sort of sharing would facilitate getting ahead of the curve in response to, for instance, a wide set of cyberspace operations aimed at distributed national infrastructures or the various weapons of a modern military – especially if the attackers are hitherto unknown, unidentified, or are using a fresh set of tools, tactics, and techniques. Indicators of systems distress may also merit passing around to accelerate immune

reactions. Other forms of learning could include: cost-effective practices (as opposed to best practices which are often unaffordable or not cost-effective for given levels of risk) and indicators of cybersecurity software effectiveness, or architectural vulnerabilities in common software or well-used access controls. And perhaps needless to add, learning, to be useful, must imply doing – implementation, monitoring, enforcement, and maintenance.

Concluding observations

The cybersecurity ideal is a network regime that can ward off attacks without having to do anything different because its architecture is already hardened against all serious attacks.

But, given the state of technology, human nature, and today's peacetime threat levels, such hardness may not be cost-effective. A second-best strategy is to foster a global system – which exists today only in rudimentary form – built from the cybersecurity community writ large that can detect nascent cyberattacks, gather indicators of such activity elsewhere, understand the vulnerabilities that permitted them to work, create countermeasures, and ensure they are implemented diligently and correctly. Although there is a cybersecurity community, its members respond to different incidents and different incentives – e.g., profit for private contractors, equities for government agencies, and prestige for individual white-hat hackers. So, it is largely up to organizations and states themselves, even if assisted by cybersecurity contractors and capacity-builders, to develop their own capacity to meet incipient and ongoing cyberattacks. As noted, their diligence varies: some are proactive, some are efficiently reactive, and others just lag.

We have argued above that in cyberspace, time is the critical variable – playing the role that distance does in kinetic domains. Attackers struggle to implement their attacks before their efforts are detected. Defenders struggle to recognize attacks so as to thwart them before attackers have succeeded completely. To move faster in the struggle is one must learn – and thereby evolve – faster than the other side does. Putatively, each side in the contest can employ strategies to retard the other side's ability to learn: e.g., the attackers can use obfuscation; the defenders, honeypots. But unless these are features of the attacker's toolkit or the defender's architecture that precede the immediate struggle, they are unlikely to emerge during the immediate contest itself. For defenders, the contest is played at the global level via software and the local level via network management. Furthermore, there are immediate responses, such as e.g., patches, selective isolation, and long-term responses, e.g., less permissive software architectures, and less permissive network architectures.

We therefore contend that if one were to model the struggle for cyberspace, the best place to start would be to use a model that places the initiative in the hands of the attacker, posits some likelihood of success, and then develops plausible response mechanisms that can be likened to immune responses. Exactly how to put numbers on any of the necessary parameters is a far more difficult question, but at least it helps to understand the basic feedback dynamics. Separate considerations need to be made for military organizations, in large part because they are under threat by enemies rather than opportunists, and because the consequences of failure are greater for them. Conversely, the best militaries have become systematic learning organizations – if circumstances allow them the luxury of time.

With the usual maxim, and caveat that all models are wrong, but some are useful (Box, 1976), we offer the following conclusions and recommendations to not only preserve cyber- but also international peace and security.

Decisions to explore and implement this or that measure, countermeasure, and so on should be mindful of the reactions carried out by the other side. If the need is quick and not

expected to recur, long-term reactions may not matter much. Otherwise, it helps to project what the offence–defence contest looks like *after* these cycles play out.

Similarly, it is best not to overcommit organizational structures or doctrines (e.g., ‘persistent engagement’ (Doubleday, 2018)) that presuppose the long-term success of measures when there are potential countermeasures that can vitiate that success. Starting a shooting war based on the belief that some cyberattack measure will promise continued success is a foolishness in its own unique class.

Likewise, the decision to carry out cyberspace operations should be mindful of the defensive and offensive countermeasures that they may induce. Although the one-time-use characteristic of zero-day exploits is well-understood, the admonition is more general: *any* notable operation will prompt general countermeasures, particularly among potential targets of the specific attacker.

Cyberspace operations carried out in order to learn what works – not just technically, but in terms of strategically useful effects – are part of the attackers’ learning processes. Countries interested in cybersecurity should discourage such activities. This raises the question of whether doing so would require reacting to failed attacks as they would to successful ones – when the former provide far less information about attribution, purpose, and whether the damage from success would have crossed the target state’s threshold for a response. Another problem is that one country, for the sake of argument, say China, may pick on another, e.g., Taiwan, as a way of sharpening its tools before trying them out on the true target, in this hypothetical scenario, the United States (Gold, 2018; Follain, Lin & Ellis, 2018).

Policies to accelerate learning can be helpful. Information sharing is one – but it helps more if such sharing is understood to be a feedstock for a knowledge base on cost-effective cybersecurity practices. Knowledge of cybersecurity is shared in the sense that it is embedded in the practices of organizations and states, in the tools they employ to pursue their policies, and the tools they use in their day-to-day operations. Even when organizations cannot or will not learn on their own, what they should have learned could be incorporated in their tools presented to them.

As bad as the cyberspace environment is today, it could become much worse very quickly. Right now, large countries capable of resourcing talented cyberwarriors have little motive to trash commercial, industrial or governmental systems and networks when persistent cyber-espionage is more worthwhile. Actually, North Korea’s campaign against South Korea may have been the only example closest to all-out cyberwar. But in a crisis or conflict, governments may lose their inhibitions and potentially justify their cyberspace operations as part of a strategic warfare campaign. Assaults would come more quickly, and the need to learn and adapt quickly would have to keep pace. Forethought about what organizational and national policies would facilitate such adjustment would help.

References

- Bowden, M. (2011) *Worm: The First Digital World War*. New York, Atlantic Monthly Press.
- Box, G. (1976) Science and Statistics. *Journal of the American Statistical Association*. 71: 791–799.
- Crowdstrike (2016) Use of Fancy Bear Android malware in tracking Ukrainian field artillery units. Available from: www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf [accessed 5 January 2019].
- Doubleday, J. (2018) CYBERCOM chief calls for ‘persistent engagement’ in advance of new cyber strategy. Available from: <https://insidedefense.com/daily-news/cybercom-chief-calls-persistent-engagement-advance-new-cyber-strategy> [accessed 5 January 2019].
- FireEye (2015) Statement for the Record Richard Bejtlich Chief Security Strategist FireEye, Inc. Before the U.S. House of Representatives Committee on Energy and Commerce Subcommittee

- on Oversight and Investigations Understanding the Cyber Threat and Implications for the 21st Century Economy.
- FireEye (2017) Presentation by Tony Cole, Global Government CTO of FireEye. *CyberWeek*, Tel Aviv (27 June).
- Follain, J., Lin, A., & Ellis, S. (2018) China ramps up cyberattacks on Taiwan. Available from: www.bloomberg.com/news/articles/2018-09-19/chinese-cyber-spies-target-taiwan-s-leader-before-elections [accessed 30 September 2019].
- Franceschi-Bicchierai, L. & Cox, J. (2018) They got ‘everything’: Inside a demo of NSO group’s powerful iPhone malware. Available from https://motherboard.vice.com/en_us/article/qvakb3/inside-nso-group-spyware-demo [accessed 5 January 2019].
- Gasperre, R.B. (2008) The Israel ‘E-tack’ on Syria: Part II. Available from www.airforce-technology.com/features/feature1669 [accessed 5 January 2019].
- Gold, M. (2018) Taiwan a ‘testing ground’ for Chinese cyber army. Available from: www.reuters.com/article/net-us-taiwan-cyber-idUSBRE96H1C120130719 [accessed 5 January 2019].
- Gooden, D. (2017) Failure to patch two-month-old bug led to massive Equifax Breach: Critical Apache Struts bug was fixed in March. In May, it bit ~143 million US consumers. Available from: <https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/> [accessed 5 January 2019].
- Gordon, L. & Loeb, M. (2002) The economics of information security investment. *ACM Transactions on Information and System Security*. 5:4: 438–457 (November).
- Greenberg, A (2018) Stealthy, destructive malware infects half a million routers. Available from: www.wired.com/story/vpnfilter-router-malware-outbreak/ [accessed 5 January 2019].
- Hutchins, E.M., Cloppert, M.J., & Amin, R.M. (2010) Intelligence-driven computer network defence informed by analysis of adversary campaigns and intrusion kill chains. Available from: www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defence.pdf [accessed 5 January 2019].
- Joyce, R. (2016) Disrupting nation state hackers. Video presentation. Available from www.youtube.com/watch?v=bDjb8WOJYdA [accessed 5 January 2019].
- Libicki, M. (2016) Defending against attacks of high and broad consequence. In Libicki, M. (2016) *Cyberspace in Peace and War*. Annapolis, MD, Naval Institute Press, pp. 59–69.
- Libicki, M. (2017) Second acts in cyberspace. *Journal of Cybersecurity*. 3(1): 29–35.
- Nolan, C. (2017) *The Allure of Battle*. Oxford, Oxford University Press.
- O’Gorman, G. & McDonald, G. (2012) The Elderwood Project. Weblog. Available from: www.symantec.com/connect/blogs/elderwood-project [accessed 5 January 2019].
- Schneier, B. (2017) Class breaks. Weblog. Available from www.schneier.com/blog/archives/2017/01/class_breaks.html [accessed 5 January 2019].
- Trend Micro (2018) A Look into the Lazarus Group’s Operation. Available from: www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations [accessed 5 January 2019].

11

CYBERCRIME

Setting international standards

Tatiana Tropina

Introduction

The threat of cybercrime has been evolving together with the evolution of the information technologies and increasing use of the information and communication networks. The last two decades have witnessed a dramatic change in the cybercrime landscape. From its early days, when computer crimes required technical skills and were committed mostly out of curiosity or to test the system vulnerabilities, digital crime grew in its scope and transformed in a complex highly sophisticated illegal industry, adopting every technological innovation to its benefit (McAfee, 2018: p. 3; Tropina, 2013: p. 52). Despite all the efforts of international organizations, governments, law enforcement agencies and industry to tackle the problem of cybercrime, it continues growing to a scale that represents a potential threat to global economic integrity (Cilluffo, 2017: p. 5).

Effective prevention, disruption, and investigation of cybercrime requires a wide variety of measures, which should combine legal frameworks, technical and organizational responses, personal safeguards, and education and awareness raising. It is widely accepted that due to the transborder nature of cybercrime it is necessary to harmonize criminal laws and procedural frameworks to avoid criminal safe havens, to carry out cross-border investigations, and to collect electronic evidence. However, when this conventional wisdom meets reality, the international community appears to be struggling to find working solutions to attain such harmonization. While developments of the frameworks to tackle cybercrime have been central to the agenda of many international organizations, the hope for a global and universal solution has been slowly vanishing in the last decade. The current state of international legal instruments addressing the problem of cybercrime and digital investigations could be characterized as a patchwork of regional, or sometimes even national unilateral solutions.

This chapter explores various efforts to harmonize cybercrime frameworks on the regional and global level. However, to do so, it firstly puts cybercrime legal frameworks into a broader context of various streams related to international norm-making in cybersecurity. The chapter starts with providing for a distinction between different domains of cybersecurity, such as national security, military defence and criminal justice, with cybercrime belonging to the latter area. It further sets the scene for the analysis of international efforts in the area of criminal justice in cyberspace by providing insights into the debate on the

definition of the term ‘cybercrime’. The second part of the chapter argues that despite all the calls to harmonize cybercrime legal frameworks, the current state of international standards represents a complex system of rather fragmented solutions. The third part analyses particular cases of intergovernmental organizations, such as the Council of Europe and the United Nations, in developing international standards to harmonize cybercrime-related legislation. It discusses the tensions between different efforts to harmonize the standards and explains why the attempts to find a ‘global’ solution on the level of the United Nations have been unsuccessful. The last part of the paper provides a brief insight into self- and co-regulatory initiatives to tackle cybercrime, arguing that public-private cooperation approach has its limitations and there is still a need for harmonized legal frameworks. The chapter concludes with summing up the current state of play and suggesting a possible way forward.

Cybercrime: definitions and blurring borders

Cybercrime in the context of international cybersecurity

The transnational nature of cyberspace and complexity of cybersecurity threats blur distinctions that were previously made between regulatory domains of civil defence, military defence, and law enforcement for the purpose of criminal justice (Bendiek, 2012, p. 6). Cyberspace dramatically changed the concepts of aggression and crime. Traditionally, the notion of aggression referred to the acts committed in the physical world for both crimes and war. The distinction between the two was unambiguous: the act of war could be clearly attributed to a nation-state (Brenner, 2007, p. 403), while the cases of breach of criminal law undoubtedly belonged to the domain of criminal justice with the aim to prosecute the offender and with the ultimate dominance of reactive approach (Watney, 2012, p. 62). However, the anonymity of cyberspace and the availability of the same tools to different malicious actors blur the borders between criminal acts and security threats coming from the nation states. Various actors can have the same target but attack it for different purposes: for example, the banking sector could be targeted by criminal organizations for financial gain and by nation state proxies for cyber-espionage (Cilluffo, 2015, p. 3). Tools, such as ransomware, could be utilized by cybercriminals to extract money from the victims and by state-backed actors to test their cyber-capabilities and resiliency of the adversary (Walters & Muller, 2017). Furthermore, malicious actors can blend together, cooperate, strengthen each other’s cyber-capabilities and use each other activities as a cover (Department of Defence, 2015, p. 9). A nation state can use organized cybercriminals to act upon its interests (Shimeall, 2016, p. 548; Cilluffo, 2015, p. 2) or collaborate with politically motivated actors, such as hacktivists, to mutual advantage.

In theory, the distinction between cybersecurity domains can be made based on the nature of threats and approaches to address them. One of the ways to draw a line is the ‘two-stream’ model suggested by Maurer (2011). His research differentiates two international approaches to the cybersecurity issues on the level of such intergovernmental organizations as United Nations: politico-military stream and economic stream. The former includes the use of the information technologies for undermining international stability and the latter refers to the criminal misuse of information technologies (Maurer, 2011, p. 6). A similar distinction can be found in other research: for example, Jang and Lim (2012, p. 7) discuss two main common approaches to the cyber-threats: security-oriented approach that considers cyber-attacks as a threat to the national security, and law enforcement approach, which brings the malicious acts to the domain of criminal justice.

However, in practice, the attribution of a particular act in cyberspace to one or another domain very poorly fits the conventional distinction between mandates in criminal justice, national security and public international law (Bambauer, 2012, p. 595). Assigning cyber-threats to one of those domains will always depend on a complex of factors, such as motivations of malicious actors, the goals of the attribution, seriousness of the threat, availability of political and legal tools for deterrence, the political landscape, and many others.

This complexity, however, means that it is more crucial than ever to clearly distinguish the domain of criminal justice. Responses to a cybersecurity threat posed by a particular type of malicious actor, however effective they might be, in many cases cannot be utilized to successfully tackle the other. Nation states hostile operations in cyberspace cannot be deterred with the same methods that are used to respond to the threat of organized cybercrime or terrorist use of the Internet: for the latter law enforcement should be equipped with appropriate frameworks for digital investigations, while the former refers to defence and national security and, in case of a serious attack, raises the issue of the applicability of international humanitarian law (Sommer & Brown, p. 11). Failure to separate the domain of criminal justice from other cybersecurity domains can lead to confusion and significant delays in developing effective responses to criminal acts committed in cyberspace. To analyze international and regional frameworks that aim to tackle the problem of cybercrime, this chapter further focuses only the international legal and policy efforts which can be clearly attributed to the development of international standards in the area of criminal justice.

Defining cybercrime

Even though the efforts to set international standards to fight crime in cyberspace have a history of at least three decades, there is no commonly held definition of cybercrime. International instruments, such as Council of Europe Cybercrime Convention and others, while using the generic term ‘cybercrime’ do not provide for a precise definition. The reason is quite simple: there is actually no need for one because the term ‘cybercrime’ should be flexible depending on the context it is used in.

When it comes to particular illegal acts that constitute the core of digital crime, most of the international and regional instruments refer to the crimes against confidentiality, integrity, and availability of computer data and systems, computer-related crimes such as computer fraud and forgery, illegal content, and child abuse crimes. Such a narrow list of acts results from the requirement of the principle of legal certainty in substantive criminal law: the definition of criminal conduct should be very specific concerning certain individual unlawful acts that entail criminal responsibility.

However, nowadays almost any crime, not only cybercrime, can leave digital traces. The law enforcement agencies use procedural frameworks that have been at first developed for investigating cybercrime to access the digital evidence for the cases of murder, robbery, drug trafficking, and many other crimes. Therefore, in the context of criminal procedural frameworks, the term “cybercrime” should be sufficiently broad to ensure that legal frameworks and international cooperation mechanisms initially developed for the purpose of collecting digital evidence in cybercrime cases will be applicable to any criminal investigations involving digital component. This would also guarantee effective safeguards and protection of privacy and other fundamental rights equally in all the types of criminal investigations in cyberspace (UNODC, 2013, pp. 21–22).

International approaches to cybercrime: a patchwork of regional solutions

It has been widely recognized that due to the transborder nature of digital crime no state can feel safe in cyberspace even if it has adopted perfect cybercrime legislation while there are countries with weak cybercrime laws or lack of capacity to investigate and prosecute digital infringements. Criminals in cyberspace can easily bypass the national legal frameworks by operating from anywhere in the world without being physically present at the crime scene. Therefore, the development of harmonized legal standards to criminalize certain acts in cyberspace as well as provide investigation tools for collection of digital evidence is the key in tackling the problem of cybercrime (Goodman, 2010; Sieber, 2008).

The calls for harmonization of cybercrime laws started as early as in 1986 when the OECD suggested the list of acts that could be used as a common denominator to harmonize approaches to the criminalization of computer crime (OECD, 1986). However, more than three decades later, the common denominator has not been found yet: legal frameworks tackling the problem of cybercrime, especially in the area of digital investigations, are highly fragmented and involve many international and regional organizations setting the standards in this field. Despite almost a global success of the most well-known and undoubtedly the most important international standard up to date – the Council of Europe's Convention on Cybercrime adopted in 2001 (the 'Budapest Convention') – many organizations, such as European Union, the Commonwealth of Independent States, African Union, the League of Arab States and others developed their own binding and non-binding regional frameworks in addition to, and sometimes instead of joining the Council of Europe treaty.

Those instruments include such frameworks as the EU Directive on Attacks Against information systems (and earlier, the EU Framework decision), the Commonwealth Model Law on Computer and Computer Related Crime, frameworks of Commonwealth of Independent States and the Shanghai Cooperation Organization, the League of Arab States' Model Law and Convention on Combating Information Technology Offences, African Union Convention on Cybersecurity and Data Protection 2014, International Telecommunication Union (ITU)/Caribbean Community (CARICOM)/Caribbean Telecommunications Union (CTU) Model Legislative Texts on Cybercrime, e-Crime and Electronic Evidence (2010), and International Telecommunication Union (ITU)/Secretariat of the Pacific Community Model Law on Cybercrime (2011) (UNODC, 2013, p. 64). All of them have to the large degree influenced each other, with the prominent role played by the Council of Europe Cybercrime Convention. However, despite having common core legal provisions, the instruments differ in substantive areas: while most of them cover the criminalization of certain illegal behaviour in cyberspace, very few – only the Council of Europe Convention, the Commonwealth of Independent States Agreement, and the League of Arab States Convention – try to establish mechanisms for international cooperation in cybercrime investigations, even though such cooperation is crucial for obtaining digital evidence quickly.

Furthermore, outside of the frameworks of setting legal standards, harmonization of operational capacities and confidence-building measures to foster collaboration in cybercrime investigations has been on the agenda of different international organizations and agencies. They include G8 Group of States, the Organization of American States (OAS), Asia Pacific Economic Cooperation (APEC), the Organization for Economic Co-Operation and Development (OECD), the Association of South East Asian Nations (ASEAN), Interpol and Europol with all of them working on facilitation of international cooperation, awareness raising and capacity building to tackle cybercrime.

However, despite all the ‘flurry of activity in relation to cybercrime at the international, regional and national level’ (Clough, 2014, p. 730) happening in the last decades, no international instrument has been widely considered as a universal solution. There are only two intergovernmental organizations that attempted to develop the instruments to harmonize cybercrime legislation beyond the regional level – the Council of Europe and the United Nations. While the Council of Europe, albeit being a regional organization, managed to advance its Cybercrime Convention far beyond the borders of Europe to be the most prominent international instrument, the efforts of the United Nations to set universal standards in fighting digital crime have not been successful so far. even though the United Nations seemed to be the most obvious platform for the development of a global solution, it has not managed to take the lead in the area of cybercrime frameworks because of, as it is argued later, the shortfall of political willingness, the lack coordinated efforts, and also due to the pioneering role of the Council of Europe in this field.

Harmonization of cybercrime frameworks: developing a global framework?

Budapest Convention: the role of Council of Europe in standards setting

The Council of Europe Convention on Cybercrime was signed in Budapest in 2001, following several years of the preparatory work, and entered into force in 2004. The Convention deals with three pillars of harmonization of cybercrime-related frameworks: criminal law, the law of criminal procedure and mutual legal assistance. It lists the number of offences that the parties are required to transpose into their domestic criminal law, such as illegal access, illegal interference, computer fraud and others. Furthermore, it provides for a number of procedural instruments tailored to the specific needs of digital investigations and calls for international collaboration in cybercrime investigations ‘to the widest extent possible’ by outlining the principles of mutual assistance when specific measures related to digital investigations are used. The Convention also contains general norms on jurisdiction and extradition in cybercrime cases.

The structure of the Budapest Convention that covers all the areas related to cybercrime legislation – from criminalization to mutual legal assistance and safeguards in criminal investigations – makes it the most comprehensive and the most widely accepted existing international standard on fighting cybercrime. As of May 2019, it has been ratified by 63 states with only three signatories not followed by ratification. Despite being developed by a regional organization, from the very beginning the Convention was open to signatures by non-member states: even during the negotiations phase, four of them – the United States, Canada, Japan and South Africa – participated in the drafting process and signed the Convention. Except for South Africa, they also ratified it. Furthermore, the list of non-members of Council of Europe that ratified the convention includes, for example, Australia, Dominican Republic, Colombia, Israel, Mauritius, Panama, Ghana (CoE, 2016).

Right after its adoption, the Budapest Convention was debated against for lacking safeguards and mechanisms to protect human rights, for creating uncertainty with regard to dual-use instruments that can be utilized by both criminals and security specialists, and, ultimately, for being only a regional instrument (Harley, 2010; Marion, 2010; Gercke, 2012, p. 124). However, despite all the criticism, the Convention has gone far beyond the borders of the region and has reached almost a global scope. It also to a high degree influenced

all other regional binding and non-binding frameworks: for example, the Commonwealth model law on cybercrime was drafted close to the Convention and was approved only after the adoption of the Council of Europe treaty. According to the UNODC Comprehensive Study on cybercrime, even those countries, which didn't formally join the Convention, used its standards in drafting the new legislation on cybercrime (UNODC, 2013; Clough, 2014).

Nevertheless, the opponents of the Convention have argued that since it was drafted by the regional organization, many countries in the world would be reluctant to join the treaty because they didn't participate in the drafting process (Clough, 2014, p. 724; Gercke, 2012, p. 125). Some of the critics also debated that the Convention was drafted mostly for developed countries and didn't take into account the needs of developing states (Gercke, 2012, pp. 126–127). Countries like Russia argued that the treaty endangers the principle of state sovereignty (Markoff & Kramer, 2009). A decade after the adoption of the Budapest Convention, the calls for 'global' framework by its opponents prompted the United Nations to launch in 2010 a global Comprehensive Study on Cybercrime in an attempt to take the lead in the process of establishing international standards and to offer an alternative solution that could potentially suit both the Council of Europe Cybercrime Convention signatory states and its most consistent critics.

United Nations: fragmented efforts

The United Nations had cybercrime on its agenda well before the commencement of the Comprehensive Study on Cybercrime: the Resolution of the General Assembly 55/59 of 2001, granted a special mandate to the Commission on Crime Prevention and Criminal Justice to develop responses to cybercrime. Digital crime has been a subject of several resolutions of the General Assembly (UNGA) and Economic and Social Council (ECOSOC) and in the WSIS Geneva Declaration of Principles and Plan of Action of the World Summit on the Information Society 2003, which called governments and the private sector to prevent, detect and respond to cybercrime and misuse of information and communications technologies. However, compared to Council of Europe's and other regional organizations' efforts in the area of crime in cyberspace, the United Nations lagged behind in taking coordinated actions that could lead to the setting of international legal standards.

Within the structure of the United Nations, cybercrime was falling under the domain of several structures, with the ITU and UNODC being the most prominent players in this field. ITU got involved into cybercrime-related efforts under the mandate of the WSIS, when it was nominated as a sole facilitator of the Action Line C5, dedicated to building confidence and security in the use of ICTs. During WSIS Forum 2009 ITU presented two tools aimed to advance its activity in tackling the problem of cybercrime: a publication 'Understanding Cybercrime: A Guide for Developing Countries' (Gercke, 2009) and an ITU Toolkit for cybercrime legislation (ITU, 2010). For the latter, ITU as a telecommunications standards-setting body faced some criticism for overstepping its mandate and entering the domain of developing legal frameworks (Gercke & Tropina, 2009, p. 139). Some of the suggestions for cybercrime laws offered by the Toolkit significantly diverted from existing international frameworks on cybercrime. As it was argued, the Toolkit could possibly be useful for developing countries as a model for drafting the laws, but it could hardly create proper legal standards (Gercke & Tropina, 2009, p. 140). Despite the failure of the Toolkit, ITU continued pursuing the projects on offering model cybercrime laws for developing countries, but in a more targeted way: from 2008, ITU together with the EU carried out several projects on drafting model legislative texts, including model texts on cybercrime, for African, Caribbean and Pacific Island Countries (ITU, n/d).

In parallel to the work of the ITU, another UN agency – UNODC – entered the field of cybercrime legal frameworks under its mandate in the area of crime prevention and criminal justice. In its Resolution 65/230 of 21 December 2010, the General Assembly requested the Commission on Crime Prevention and Criminal Justice to establish an open-ended inter-governmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime (UNGA, 2010). In May 2011 UNODC and ITU signed a Memorandum of Understanding to join efforts in capacity building, offering member states assistance in four key areas: assessment, review of legislation, technical assistance and capacity building (ITU/UNODC, 2011).

UNODC Comprehensive Study on Cybercrime: a failed call for a 'global' solution

The Comprehensive Study on Cybercrime, which was carried out by the UNODC upon the request of General Assembly, has been of the most significant efforts on harmonising cybercrime legislation taken by the UN on the global level. The UNODC methodology for the study included the distribution of a questionnaire to the Member States, intergovernmental organizations and representatives from the private sector and academic institutions and further analysis based on the responses and additional research (UNODC, 2013a). The work was carried out in 2011–2013 and included significant efforts on collecting analysing legislation, statistics and responses to the questionnaire. The result of the study, published in February 2013 as a draft (UNODC, 2013a), represented probably the most comprehensive snapshot of the state of cybercrime and cybercrime legislation globally.

The study concluded that there was still fragmentation at the international level and among the nation states concerning the cybercrime legislation and that international cooperation in digital investigations yet relied on traditional means of the mutual legal assistance, which were not always able to address the issues timely. Furthermore, it called for capacity building and awareness raising, public-private partnerships and the integration of cybercrime strategies into a broader cybersecurity perspective. It also suggested several options to strengthen existing and to develop new national and international legal and other responses to cybercrime, with most of them assuming a greater role of the United Nations in setting international standards in this area. The suggested options included the international model provisions on the criminalization of core cybercrime acts, international model provisions on investigative powers for electronic evidence, and model provisions on jurisdiction or electronic evidence. Ultimately, one of the suggested options was to draft a comprehensive multilateral instrument on cybercrime on the level of the United Nations (UNODC, 2013b).

The outcome of the study and its recommendations were discussed at the second meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 25 to 28 February 2013. At the meeting, despite all the efforts of the UNODC to reach an agreement on options related to the intergovernmental legislative solutions, the member states were not able to come to any consensus in this regard due to the resistance of the countries that had already joined the Council of Europe Cybercrime treaty and were concerned that the UN-developed solutions will lower the standards set by the Budapest Convention. The report from the meeting noted that 'diverse views were expressed regarding the content, findings and options presented in the study' (UNODC, 2013b) and the only recommendations that reached a broad agreement were those to support the role of the UNODC in capacity building

and technical assistance and to forward the study for the consideration of the Commission on Crime Prevention and Criminal Justice. The results of this meeting are reflected in the Resolution 22/8, passed at the 22nd Commission on Crime Prevention and Criminal Justice, which abandoned any hope for a global treaty and focused only on further actions related to capacity building, technical assistance and public-private cooperation (UNODC, 2010).

Being a significant and ambitious undertaking, in the end the UNODC Study has reached its aims only with regard to providing the global picture of the problem of cybercrime in the UN-member countries and taking yet another step, among many others on the international level, in strengthening capacity to tackle the problem. However, all the efforts of the UNODC to use the Study and its results as a framework for further negotiations on the global cybercrime legal standards fell flat. The main reason was that UNODC tried to position itself in the field too late, and, therefore, was unable to compete with the success of the Council of Europe Convention. After 12 years after the adoption of the Budapest treaty the Council of Europe enjoyed a very strong support with its members providing a great resistance to the development of any competing instrument, and the UNODC was not able to get enough capacity to mobilize the member states to overcome the political differences.

Six years after UNODC Cybercrime Study: harmonization without harmonization

Since the failure of the Comprehensive Cybercrime Study to prompt the negotiations of the new cybercrime instruments, UNODC hasn't taken any significant attempts to reinforce its suggestions for the global legal treaties in this field. This might have contributed to further success of the Cybercrime Convention, which since 2013 has been ratified by more than 15 of the non-members of Council of Europe.

The lack of success of the UN attempt to set the standards for further harmonization of cybercrime frameworks had no negative effect on the substantive criminal law, which provides the standards for the criminalization of certain acts. Regional solutions were drafted closely enough to each other and to the Budapest Convention, therefore, the national approaches to what constitutes cybercrime are to a large degree unified, except some areas of disagreement such as content crimes, that have a very little chance to ever be harmonized due to different national attitudes to freedom of speech or to the definition of harmful content. Thus, even in the absence of a globally accepted solution, most of the countries have adopted cybercrime legislation to meet the dual criminality requirement that is necessary for international cooperation in investigating and prosecuting cybercrimes.

However, the regional solutions, including the Council of Europe Convention and other instruments have not yet solved the problem of harmonization of procedural instruments and international cooperation in criminal investigations to a degree that would allow a fast transborder data exchange. Mutual legal assistance instruments are still slow and inefficient and cannot sufficiently address the crucial need to obtain data quickly (Maillart, 2018). Meanwhile, the problem of the lack of procedural instruments for mutual legal assistance in collecting electronic evidence has already gone far beyond the scope of cybercrime investigations with many crimes, especially serious crimes, requiring digital investigations. While Council of Europe and the parties to the Cybercrime Convention since 2017 have been working on the Second Additional Protocol to address the challenges of international cooperation in collection of electronic evidence, the current lack of regional and international mechanisms prompted national legislators and regional organizations to develop unilateral solutions to solve the problem of obtaining data stored abroad. The recent two

years witnessed solutions emerging on both sides of the Atlantics. The United States adopted the CLOUD Act (Clarifying Lawful Overseas Use of Data Act), which would allow the US and – under bilateral agreements – foreign law enforcement to extraterritorially request the data from the providers directly without the use of the traditional mutual legal assistance mechanisms. The European Union is working on the set of controversial proposals related to the collection of electronic evidence to allow for direct cross-border requests for data in criminal investigations without the national judicial approval in the executing state required under the mutual legal assistance regime (EC, 2018). Both the US CLOUD Act and the EU E-Evidence regulation proposals have been heavily criticized for potentially lowering the existing standards of fundamental rights protection (Böse, 2018, p. 46), privatising law enforcement (EFF, 2018; ETNO, 2018; EuroISPA, 2018), and turning intermediaries into de-facto judicial authorities (EDRi, 2018). However, the lack of harmonized approaches to electronic evidence collection would probably lead to further unilateral solutions and fragmentation – it is highly likely that once both US and the EU will start applying the provisions on direct requests for data stored abroad, the third countries would follow the precedent and adopt a similar legislation (CISPE, 2017, p. 2; DigitalEurope, 2018, p. 1).

Public-private collaboration in tackling cybercrime: complement, not privatize

In the absence of truly harmonized global standards to for investigation of cybercrime, the governments and law enforcement agencies put great faith in the voluntary involvement of the industry and public-private cooperation as a part of broader efforts to approach cybersecurity from the multi-stakeholder perspective. The involvement of business, civil society and technical community in fighting cybercrime started as early as in the 1990s with the establishment of private reporting platforms and hotlines for reporting illegal content. The first initiatives include the UK's Internet Watch Foundation (IWF) – a private industry-based self-regulatory body that launched a hotline for reporting online child-abuse content in 1996 (Akdeniz, 2001, p. 307) and the pan-European hotline association INHOPE, which was established in 1999 in order to coordinate reporting of illegal content and expanded in Europe in the beginning of the 2000s (Marsden, Simmons & Cave, 2006). In the last twenty years, collaboration to tackle illegal content evolved and resulted in the adoption of the voluntary codes of conducts for the ISPs, in particular, those regulating notice-and-takedown procedures. Business, technical community and civil society have been involved in various efforts, such as in user's safety public awareness campaigns (Cisco, 2010, p. 27), school education (Choo, 2009), law enforcement training, and capacity building programs for financial institutions to detect suspicious transactions (Choo, Smith & McCusker, 2007, p. 94), to name a few. The major operations in tackling complex crime online, such as botnet takedowns and dismantling organized cybercrime networks have become a track record of successful cross-border cooperation between the law enforcement agencies, industry and technical community (Europol, 2016; Europol, 2017).

While this collaboration is essential and important, it is crucial to understand that public-private cooperation in cybercrime is not able to substitute proper legal frameworks and it was never meant to do so. Criminal investigations always require a strong involvement of public authorities (Malmström, 2012, p. 2). Criminal law is the sole domain of national governments and law enforcement agencies, it involves not only criminalization of certain acts but also strict frameworks of court authorization for particular procedural measures, control and oversight. It cannot and shall not be privatized (Tropina & Callanan, 2015, p. 19; ETNO, 2018; EuroISPA, 2018). Due to the uniqueness of the law enforcement mandate

and the nature of criminal law, public-private collaboration can help to prevent, disrupt or attribute criminal acts in cyberspace, but it will never substitute the proper legal frameworks because only law can guarantee the proper crime investigations and prosecution of offenders in the transborder environment (Gercke et al., 2011). The power to enforce rules in the field of criminal law is limited to the governments and has to follow very strict safeguards and procedures, because of the human rights protection component involved in criminal investigations. It is governments, law enforcement and judiciary who are ultimately accountable and responsible for upholding fundamental rights in digital investigation. Any collaborative approaches with industry in digital investigations represent an additional lawyer to the criminal law and should operate within strict rules that protect the rights of suspects, victims, and anyone else who can be affected in the process of digital evidence collection. Therefore, while some of the public-private efforts to prevent, detect and report cybercrime, such as awareness-raising campaigns, detection of malicious activity, takedown of botnets can have a greater degree of flexibility, when it ultimately comes to the investigation and prosecution there is always a need for criminal law, and, as a result, the need for internationally harmonized standards to ensure efficient mutual legal assistance.

Conclusion

In 2019, more than 30 years after the OECD took the first attempt to find a common denominator for the criminalization of computer crimes, nation states and international organizations are still struggling with the lack of universally accepted standards. Despite all the calls for harmonized cybercrime frameworks, the approaches to cybercrime represent a patchwork of different binding and non-binding legal instruments, traditional mutual legal assistance mechanisms and unilateral solutions that are getting more and more fragmented. The global bodies, such as the UNODC and the ITU, despite having the UN mandate to cybercrime-related activities, could not bring together different states to find a common approach to criminalize cybercrime-related acts and develop a framework for digital investigations. Is very unlikely that UN can take a lead in setting legal standards on cybercrime in any foreseeable future, and even if it could, the perspectives of negotiating a global framework within the short-term timeframe are absolutely unrealistic. Any solution of this kind will require a significant effort of reaching political consensus, which, taking into account various political interests and the existence of competing regional frameworks, would be very hard to attain.

In the absence of a globally accepted solution, the Budapest Convention is gaining more prominence and has a great potential to become a truly universal standard. However, this will happen only if Council of Europe manages to address the challenges of cooperation in digital investigations before the unilateral solutions circumventing the mechanisms of mutual legal assistance, such as the US Cloud Act, become a widely accepted practice.

Another potential solution is to further strengthen cooperation among the parties of different existing regional instruments, such as the Budapest Convention, EU frameworks, African Union Convention on Cybersecurity and Personal Data Protection and others. The involvement of Council of Europe, UNODC and the ITU in the capacity building, especially in developing countries, might greatly contribute into these efforts and leverage the good practices from the regional efforts to the international level. In the situation of the global 'harmonization' deadlock, when the political perspectives of either adoption of any cybercrime instrument by the United Nations or the universal acceptance of Budapest Convention due to political positions of some of the countries look rather unrealistic, the enhancement and development of the existing approaches look like the only way forward.

References

- Akdeniz, Y. (2001) Internet content regulation. UK government and the control of internet content, computer law and security report 17(5).
- Bambauer, D.E. (2012) Conundrum. *Minnesota Law Review*. 96(2): 584–674.
- Bendiek, A. (2012) European cyber security policy. *Stiftung Wissenschaft und Politik*, RP 13 (October). Available at: www.swp-berlin.org/fileadmin/contents/products/research_papers/2012_RP13_bdk.pdf [accessed 11 May 2019].
- Böse, M. (2018) An assessment of the Commission's proposals on electronic evidence. Study requested by LIBE Committee. European Parliament. Available at: [www.europarl.europa.eu/RegData/etudes/stud/2018/604989/ipol_stu\(2018\)604989_en.pdf](http://www.europarl.europa.eu/RegData/etudes/stud/2018/604989/ipol_stu(2018)604989_en.pdf) [accessed 12 May 2019].
- Brenner, S. (2007) At light speed: Attribution and response to cybercrime/terrorism/warfare. *Journal of Criminal Law & Criminology*. 97: 2.
- Choo, R. (2009) The organised cybercrime threat landscape. International serious and organised crime conference 2010. Available at: www.aic.gov.au/events/aic%20upcoming%20events/2010/_/media/conferences/2010-isoc/presentations/choo.pdf [accessed 11 May 2019].
- Choo, R., Smith, R., & McCusker, R. (2007) Future directions in technology-enabled crime: 2007–2009. *Res Publ Policy Ser*. 78: 61–80
- Cilluffo, F. (2015) A global perspective on cyber threats. Testimony before the US House of Representatives, Committee on Financial Services, Subcommittee on Oversight and Investigations (June 16). Center for Cyber & Homeland Security, George Washington University.
- Cilluffo, F. (2017) A borderless battle: Defending against cyber threats. Testimony before the US House of Representatives Committee on Homeland Security (March 22). Center for Cyber & Homeland Security, George Washington University.
- Cisco (2010) Annual security report highlighting global security threats and trends. Available at: www.cisco.com/c/dam/en/us/products/collateral/security/security_annual_report_2010.pdf [accessed 11 May 2019].
- CISPE (2017) CISPE Response to the public consultation on improving cross-border access to electronic evidence in criminal matters (27 October). Available at: https://ec.europa.eu/info/sites/info/files/cispe_2017_en.pdf [accessed 12 May 2019].
- Clough, J. (2014) A world of difference: The Budapest Convention on cybercrime and the challenges of harmonization. *Monash University Law Review*. 40: 3.
- Council of Europe (CoE) (2016) *Chart of signatures and ratifications of Treaty 185 Convention on Cybercrime. Status as of 30/10/2016*. Available from: www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures [accessed 11 June 2019].
- Department of Defense (2015) The DoD Cyber Strategy 2015. Available at: www.hsdl.org/?abstract&did=764848 [accessed 12 May 2019].
- DigitalEurope (2018) Digitaleurope position on the proposed e-evidence package (Brussels, 2 August). Available at: www.digitaleurope.org/resources/928/ [accessed 11 June 2019].
- EDRi (2018) EU 'e-evidence' proposals turn service providers into judicial authorities (17 April). Available at: <https://edri.org/eu-e-evidence-proposals-turn-service-providers-into-judicial-authorities/> [accessed 11 June 2019].
- Electronic Frontier Foundation (EFF) (2018) The U.S. CLOUD Act and the EU: A privacy protection race to the bottom. Available at: www.eff.org/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom [accessed 11 June 2019].
- European Association of Internet Services Providers Association (EuroISPA) (2018) Proposal for a regulation on European production and preservation orders for electronic evidence in criminal matters. EuroISPA's considerations. Available at: https://ec.europa.eu/info/law/better-regulation/feedback/12862/attachment/090166e5bc528e33_en [accessed 11 June 2019].
- European Commission (EC) (2018) 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 (17 April).
- European Telecommunications Network Operators' Association ETNO (2018) ETNO position paper on improving cross-border access to electronic evidence in criminal matters. Available at: <https://etno.eu/datas/positions-papers/2018/ETNO%20position%20paper%20on%20improving%20cross-border%20access%20to%20electronic%20evidence%20in%20criminal%20matters.pdf> [accessed 11 June 2019].

- Europol (2016). Avalanche Network Dismantled in International Cyber Operation. 01 December 2016. Press Release. www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation [accessed 11 June 2019].
- Europol (2017) Andromeda Botnet Dismantled in International Cyber operation. (4 December) Press Release. Available at: www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation [accessed 11 June 2019].
- Gercke, M. (2009) Understanding cybercrime: A guide for developing countries. Draft April 2009. Available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf [accessed 11 June 2019].
- Gercke, M. (2012) Understanding cybercrime: Phenomena, challenges and legal response. Available at: www.icao.int/cybersecurity/SiteAssets/ITU/Cybercrime%20legislation%20EV6.pdf [accessed 11 June 2019].
- Gercke, M. & Tropina, T. (2009). From telecommunication standardisation to cybercrime harmonization? ITU toolkit for cybercrime legislation. *Computer Law Review International*. 5.
- Gercke, M., Tropina, T., Lozanova, Y., & Sund, C. (2011) The Role of ICT regulation in addressing offences in cyberspace. *Trends in Telecommunication Reform 2010/11. Enabling Tomorrow's Digital World*. ITU: 187–238.
- Goodman, M. (2010) International dimensions of cybercrime. In Ghosh, S. & Turrini, E. (eds) *Cybercrimes: A Multidisciplinary Analysis*. Berlin and Heidelberg: Springer-Verlag
- Harley, B. (2010) A global convention on cybercrime? *Columbia Science and Technology Law Review* (March 23). Available at: <http://stlr.org/2010/03/23/a-global-convention-on-cybercrime/> [accessed 11 June 2019].
- International Telecommunication Union (ITU) (n/d) Support for the establishment of harmonized policies for the ICT market in the ACP states. Available at: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/Pages/default.aspx [accessed 11 June 2019].
- International Telecommunication Union (ITU) (2010) ITU toolkit for cybercrime legislation. Draft rev. (February). Available at: <https://cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf> [accessed 11 June 2019].
- International Telecommunication Union (ITU/UNODC) (2011) Cybercrime: The global challenge. Available at: www.itu.int/en/ITU-D/Cybersecurity/Pages/UNODC.aspx [accessed 11 June 2019].
- Jang, Y. & Lim, B. (2012) Harmonization among national cyber security and cybercrime response organizations: new challenges of cybercrime. 4th Asian Criminology Conference. Available at: <http://arxiv.org/abs/1308.2362> [accessed 11 June 2019].
- Maillart, J.-B. (2018) The limits of subjective territorial jurisdiction in the context of cybercrime (2018). In: ERA Forum, DOI/10.1007/s12027-018-0527-2, Forthcoming. Available at SSRN: <https://ssrn.com/abstract=3249367> [accessed 11 June 2019].
- Malmström, C. (2012) Public-private cooperation in the fight against cybercrime. EU cybersecurity and digital crimes forum, Brussels (31 May). Available at: http://europa.eu/rapid/press-release_SPEECH-12-409_en.htm?locale=en [accessed 11 June 2019].
- Marion, N.E. (2010) The Council of Europe's cyber crime treaty: An exercise in symbolic legislation. *International Journal of Cyber Criminology*. 4(1&2): 699–712
- Markoff, J. & Kramer, A. (2009) In shift, U.S. talks to Russia on internet security. *The New York Times* (December 12). Available from: www.nytimes.com/2009/12/13/science/13cyber.html [accessed 16th May 2019].
- Marsden, C., Simmons, S., & Cave, J. (2006) Options for an effective-ness of internet self- and co-regulation. Phase 1 report: Mapping existing co- and self-regulatory institutions on the internet. RAND Europe. Available at: http://ec.europa.eu/dgs/information society/evaluation/data/pdf/studies/s2006_05/phase1.pdf [accessed 11 June 2019].
- Maurer, T. (2011) Cyber norm emergence at the United Nations – An analysis of the activities at the UN regarding Cyber-security. Discussion Paper #2011-11, Explorations in Cyber International Relations Discussion Paper Series (September). Available at: <http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf> [accessed 14th May 2019].
- McAfee (2018) Economic impact of cybercrime – no slowing down. Available at: <https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf> [accessed 11 June 2019].

- Organization for Economic Co-operation and Development (OECD) (1986) Computer-related criminality: analysis of legal policy in the OECD area. Report DSTI-ICCP 84.22 (18 April).
- Shimeall, T. (2016) From cyber crime to cyber war: Indicators and warnings. In Williams, P. & Fiddner, D. (eds), *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition*. US Army War College.
- Sieber, U. (2008) Mastering complexity in the global cyberspace: The harmonization of computer-related criminal law. In Delmas-Marty, M., et.al. (eds), *Les chemins de l'Harmonization Pénale/Harmonising Criminal Law, Collection de L'UMR de Droit Comparé de Paris*. Paris, Société de législation comparée, pp. 127–202.
- Sommer, P. & Brown, I. (2011) Reducing systemic cybersecurity risk. OECD. Available at: www.oecd.org/gov/risk/46889922.pdf [accessed 11 June 2019].
- Tropina, T. (2013) Organised crime in cyberspace. In Heinrich-Böll-Stiftung/Schönenberg (eds), *Transnational Organized Crime: Analyses of a Global Challenge to Democracy*. Bielefeld, Transcript Verlag, pp. 48–60.
- Tropina, T. & Callanan, C. (2015) Self- and co-regulation in cybercrime, cybersecurity and national security. SpringerBriefs in Cybersecurity.
- United Nations General Assembly (UNGA) (2010) Resolution 65/230. (21 December).
- UNODC (2010) Resolution 22/8. Available from: www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-8.pdf [accessed 11 May 2019].
- UNODC (2013a) UNODC Comprehensive Study in Cybercrime. Available at: www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [accessed 11 June 2019].
- UNODC (2013a) Comprehensive Study on Cybercrime. United Nations, New York. Available at: www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [accessed 11 June 2019].
- UNODC (2013b) Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. Executive summary. Available at: www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf [accessed 11 June 2019].
- Walters, R. & Muller, M. (2017) State actors are likely behind recent ransomware attacks. Commentary. Available at: www.heritage.org/cybersecurity/commentary/state-actors-are-likely-behind-recent-ransomware-attacks [accessed 11 June 2019].
- Watney, M. (2012) The way forward in addressing cybercrime regulation on a global level. *Journal of Internet Technology and Secured Transactions*. 1: 3.

12

CYBERTERRORISM

A Schrödinger's cat

Mika Kerttunen

Introduction

The United Nations Security Council (UNSC) Resolution 1373 (2001) reaffirmed that ‘any act of international terrorism’ constitutes a threat to international peace and security. This post-9/11 reaffirmation followed the 1992 Resolution 731 qualifying acts of international terrorism as threats to international peace and security, and the 1999 Resolution 1269 condemning all acts, methods and practices of terrorism, regardless of their motivation and in all forms and manifestations.

The United Nations Group of Governmental Experts (UN GGE) reports (2010, 2013, 2015) have expressed growing concerns over the terrorist use of information and communication technologies. Governments (e.g. US, 2011; RU MFA, 2016) and corporations (e.g. Smith, 2017) have similarly become alarmed of terrorism in and through cyberspace. The Security Council while recognizing ‘a growing importance of ensuring reliability and resilience of critical infrastructure and its protection from terrorist attacks for national security, public safety and the economy of the concerned States as well as well-being and welfare of their population’ (UNSC, 2017a) and underlining the need to prevent terrorists from ‘exploiting technology, communications and resources’ (UNSC, 2017b), has so far not yet discussed cyber threats to international peace and security, including (see Chapter 30).

The empirical evidence of the latest terrorist attacks, from Madrid 2003 and Mumbai 2008 to Paris 2016 and Brussels 2017, rather speaks of advanced use of digital systems and services than seeking to destroy information and industrial systems by digital means. Concluding the obvious, that physically violent terrorist acts, regardless of their contextual sophistication, did not cause destructive effects in or through cyberspace is a necessary reminder of violence being and being regarded as the centrepiece terroristic *modus operandi*. This tautological conclusion leads to ask of the relevance of the very premise: can violent effects be digitally created; is it necessary for cyberterrorism to be directly violent to be regarded as terrorism; and is there beyond the clause of death-and-destruction an *Effect 2.0* that needed to be counted in? Given the omnipresence and assumed omnipotence of information and communication technologies, it is timely to critically examine whether, how, and to what extent cyberterrorism may constitute a threat to international peace and security.

Reversing this basic question is also necessary. Examining if a deficit of international peace and security writ large may trigger cyberterrorism helps to understand the broader dynamics between cyberterrorism and international peace and security.

On cyberterrorism

The talk about cyberterrorism has most often talked of hacking, propaganda or the use of ICTs to support terrorist acts (e.g. Coats 2018, p. 6). The expressed concerns more often than not have focussed on national rather than regional or global security. Moreover, as the constructivist line of cybersecurity research (especially Eriksson, 2001; Conway, 2005; Bendrath, Eriksson & Giacomello, 2006; and Dunn Cavelty, 2008) points out the claim of cyberterrorist threat is intersubjectively constituted. Similarly to Fischer's (1967) note of Soviet sociology, in cybersecurity studies as well, cyberterrorism included, official documents and political speech-acts usually constitute key evidence. In fact, before any observations, 'cyberterrorism' has come to exist in several configurations, turning out to be a cat that is simultaneously dead and alive.

Disregarding the truism that there is no conceptually, politically, or legally agreed definition of terrorism, it is possible to draw the contours of a terrorist act. Sinclair and Antonius (2013) consider the primary goal of conventional terrorism being undermining 'civilians' resilience by instilling a sense of fear and vulnerability that erodes confidence in the ability of the government and law enforcement agencies to protect citizens against future attacks'. More specific criteria of virtue and of consequences are reflected in the UNGA (1994) 'Declaration on Measures to Eliminate International Terrorism': first, the act is illegal; second, it is violent; third, it is politically motivated seeking a change; and fourth, it seeks to scare, terrorize, and intimidate. A similar approach can be found e.g. in the British Terrorism Act (HMG, 2000), which establishes a cyber-attack-terrorism linkage.

Accordingly, Denning (2000) defined cyberterrorism as 'unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives'. Applying the criteria of destruction and fear, she specified that to qualify as terrorism an attack should be violent against persons or property, including critical infrastructure, causing destruction or 'enough harm' to generate fear (p. 1).

These dictionary definitions do not make claims about the scale of the acts or their impact: e.g. how destructive or terrorizing an act is. They do not determine who is and who is not a terrorist either. Yet, paying attention to the motives and *modus operandi* of terrorism enables differentiating terrorist acts from other illegal or destructive acts, and cyberterrorism from other ways of using, harming or exploiting data, networks, and on-line services. Accordingly, Yunos, Ahmad and Yusoff (2014) suggested a framework of cyber terrorism, consisting the perspectives of motivation, target, method of attack, domain, action by perpetrator, and impact, to better understand and counter cyberterrorism (pp. 527–528).

Early 2000's academic reports and professional testimonies were not convinced how significant a threat cyberterrorism was – Denning was not, either. For example, during the 2002 US House of Representatives hearings on cyberterrorism in the context of critical infrastructure protection, Thomas stated that '[F]or the foreseeable future, acts of cyberterrorism like the ones usually imagined, will be very difficult to perform, unreliable in their impact, and easy to respond to in relatively short periods of time.' Moreover, he concluded that such an unlikely attack to succeed, the US has 'some of the best resources available to deal with it, diffuse, and neutralize such a threat' (p. 9).

Lewis (2002) questioned cyber-attacks as lucrative means for terrorists who seek shocking effects and political objectives. He emphasized how greater reliance on internet-accessible computer networks can be exploited to provide terrorist intelligence constituting a greater risk for national security than cyber-attacks (p. 9).

Weimann (2004) stated that despite no single act of cyberterrorism had taken place, its potential and alarming threat cannot be denied or ignored. He listed low costs, anonymity, wide target surface, remote execution, and impact to large number of persons as making on-line terrorism an attractive option, especially in targetting critical infrastructure. Referring to Thomas (2002) and Lewis (2002), Weimann remained sceptical how serious the threat of cyberterrorism actually is. He also highlights how the failure to differentiate hacking and cyberterrorism has exaggerated the threat. Dunn Cavelty (2008) regarded deadly and destructive cyber-attacks 'largely the stuff of Hollywood movies or conspiracy theory' (p. 20).

According to Jarvis, Macdonald and Nouri's (2014) survey-based analysis established 'no meaningful consensus' existed within global research community as to whether cyberterrorism posed 'a security threat; the potential targets of cyberterrorist attacks; or, indeed, whether cyberterrorism has even yet occurred' (p. 83). Gross, Canetti and Vashdi (2017, p. 56) conclude that threat perception and not just actual cyber events created the cognitive effects of cyberterrorism.

The UN Groups of Governmental Experts have noticed terrorists using ICTs in their activities. The GGE 2010 report stated that 'at the present time terrorists mostly rely on these technologies to communicate, collect information, recruit, organize, promote their ideas and actions, and solicit funding', and that 'thus far', there had been 'few indications of terrorist attempts to compromise or disable ICT infrastructure or to execute operations using ICTs'. The Group considered such attempts may intensify in the future, that terrorists 'could eventually adopt the use of ICTs for attack' (#6). The 2013 report spoke of the possibility of terrorist groups acquiring attack tools enabling them to carry out disruptive ICT activities (#7). The 2014–2015 Group made an important connection as it recognizes how '[t]he use of ICTs for terrorist purposes, *beyond* [author's emphasis] recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security' (#6).

United Nations Office for Drug and Crime (UNODC) (2012) report introduced a functional approach, classifying the means by which the Internet is often utilized to promote and support acts of terrorism. UNODC vertically discussed six 'sometimes overlapping categories': propaganda (which includes recruitment, radicalization and incitement to terrorism); financing; training; planning (utilizing secret communication and open-source information); execution; and cyberattacks (pp. 3–12). It should be noted that the category of execution refers to ICT enabled measures to support the terrorist act, not to the act itself. Furthermore, the report observes that 'cyberattacks may bear the characteristics of an act of terrorism,' including instilling fear and furtherance of political or social objectives but considers the topic being beyond its scope (p. 12).

The Group of Seven 'Taormina Statement on the Fight Against Terrorism and Violent Extremism' (2017) and the Group of Twenty 'Action Plan on Countering Terrorism' (2017) recognized the misuse of the Internet by terrorists, including propaganda, financing and on-line recruitment but do not examine destructive use of ICT, (G7: #5; G20: #20) the aspect of 'beyond' the 2015 GGE report mentions and the BRICS (2015: #34) implicitly hints to in their otherwise strong condemnation of terrorism.

Similarly, national cyber security strategies quite vaguely speak of terrorism. For example, the French 'Digital Security Strategy' (French Prime Minister, 2015) noted dissemination of

propaganda ‘to attract volunteers and terrorise the populations’ (p. 38); the British Cyber Security Strategy (HMG, 2016) assessed the current technical capability of terrorists is judged to be low, states terrorist groups continuing to aspire to conduct damaging cyber activities, and considers even low-sophistication activities enable terrorist groups to attract attention and intimidate their victims (p. 19); the Philippines ‘Cybersecurity Plan’ (2016) mentioned recruitment, low sophisticated disruptive activities (‘defacement and distributed denial-of-service attacks’) and exchange of skills (p. 15); and the Russian ‘Doctrine of Information Security’ (RU MFA, 2016) elaborated terrorists and extremist organizations using information tools to fester tensions, incite hostility, spread ideology and recruit supporters but also ‘actively develop destructive tools to impact critical information infrastructure objects’ (#13).

Whether cyberterrorism is a serious, real problem, nationally or internationally, primarily depends on the criteria applied to define terrorism. The threat of cyberterrorism, and the respective preventive and counter-measures, are justified of terrorists by default wanting to exploit also information based critical systemic vulnerabilities. The cyberterrorist threat is constructed to include e.g. botnets, malware, denial-of-service attacks and electromagnetic energy, the attack vectors hackers, cybercriminals and nation states are known to possess and to have employed. In these extrapolations, incidents such as ‘Estonia 2007’, ‘Stuxnet’, ‘Saudi Aramco’ or various Arabic ‘cyber armies’ directly or indirectly come to testify of the existence of cyberterrorism. (Weimann, 2015: pp. 154–172) Telling to our times is that Facebook, a powerhouse of social media, behavioural analysis, and advertising, has taken a stand against undesirable acts which, with notions of premeditated violence, intimidation of the population, and a political aim, follow closely the general appreciation of terrorism (Facebook, 2018).

The use of ICT for terrorist purposes includes facilitation of terrorism by propagandist purposes to radicalize and recruit target audiences but also to exercise operational command, communication and strategic, operational and tactical guidance. It also includes the currently mostly speculative employment of contemporary and future tools, technologies, and vulnerabilities to attack critical national infrastructure and industrial and societal systems. Societal boundaries of tolerable and intolerable and juridical boundaries of legal and illegal determine how these activities are being dealt with.

Indeed, network-based penetrations of, and causing destructive effects in, technical-informational systems could be recognized as terrorist acts if and when performed with the intention of policy change through intimidation. It should be noted that similar means and methods can be used for criminal purposes as well as State projection of cyber and cyber military power – yet both usually without the intention of public intimidation. Moreover, posting acts of violence can terrorize and harm civilians physically or psychologically (Gross, Canetti & Vashdi, 2017). This may change public and political opinion even without the core criteria of physical violence *en masse* directed at the public.

Maintaining the strong, narrow, death-destruction-terror and consequentialist perspective, it is fair to conclude that terrorists have not gone beyond communications, financing, incitement, and admittedly horrific propaganda in their use of ICTs. Applying an actor-focussed perspective of malicious use of ICTs cyberterrorism acquires national and international attention (e.g. Riglietti, 2016). Moreover, the discussion of technical vulnerabilities, theoretical avenues of attacks and potentially created effects occupies an extrapolative space where possible future, rather than the present, state of affairs is used as the frame of reference. Yet, even though we may conceptually and legally acknowledge certain on-line activities as cyberterrorism, this does not necessarily bridge cyberterrorism to international peace and security.

International peace and security

The notion of international peace and security refers to the United Nations as the guardian of international peace and security. The idea also refers the UN Charter Article 39, which authorizes the Security Council to determine the existence of a threat to the peace, breach of peace or an act of aggression. The Security Council does not apply any explicit criterion, but the afore-mentioned determination and decisions are affected by collective and admittedly politically motivated considerations. In its determinations, the Council has referred e.g. to repression of population, deteriorating humanitarian situation, flows of refugees, continued violence and loss of life, but also to known or projected cross border incursions and consequences to neighbouring countries. (Värk, 2009; DPA 2018; UNSC Res. 688, 841, and 1132)

It should be noted that, despite the frequent cyber incidents, some nations' urgent calls for global mechanisms to deal with international cyber or information security, and the sickening images of beheadings or other acts of brutal violence, the Security Council has not discussed cyber security or cyberterrorism.

In condemning terrorism, UNGA (1994) briefly mentioned how terrorism may threaten international peace and security. Terrorism was considered to jeopardize the friendly relations among States and peoples; threaten the territorial integrity and security of States; gravely violate the purposes and principles of the United Nations, 'which may pose a threat to international peace and security'; hinder international cooperation; and aim at the destruction of human rights, fundamental freedoms and the democratic bases of society (#1–3). Reaffirming the need of international cooperation to prevent and combat terrorism the 'United Nations Global Counter-Terrorism Strategy' (UNGA, 2006) also categorized the aims of terrorist 'acts, methods and practices' in line with the rather common determinations of threats to, and breaches of, international peace and security the Security Council has applied: the destruction of human rights, fundamental freedoms and democracy; threatening territorial integrity, security of States; and destabilizing legitimately constituted governments.

Outlining the interrelationship between terrorism and international peace and security in the context of ICTs requires and combines the three elements discussed above: the logic and *modus operandi* of terrorism [the subject]; the general claims of the vulnerabilities of ICT systems and services, in particular critical infrastructure [the object]; and the operationalization of threats and breaches to international peace and security [the impact]. The following heuristic model does not address the likelihood of such situations but functions as a conceptual framework for further analyses of cyberterrorism. The logical connections between subject, object and impact construct possible paths of development. Three paths presume acts of cyberterrorism negatively affecting international peace and security, and one, reversing the equation, considers the lack of international peace and security incentivizing cyberterrorism.

Path 1. Cyberterrorism is attributed to a state

Cyber-attacks that cause death of people, injury to people or destruction of physical objects; or create the effects of manipulation, disruption, denial, degradation, or destruction of data and are targeted against civilian population or functions are attributed to a government, government organ, or government-attributed entity. Depending of the overall context such action can be interpreted as use of force, breach of the law of non-intervention and cyberterrorism. In practise, depending on the scale of harmful effects the victim state responses vary from diplomatic measures, countermeasures, sanctions, and imposing harmful consequences to forceful responses.

Path 2. Cyberterrorism destabilizes the functionality of ICT systems and services

Cyber-attacks create disruptive or destructive effects in governmental systems or functions, critical infrastructure or essential national services with the intention to create economical loss, distrust, chaos, subversion or change of public or political opinion. The first level, technical effects created do not necessarily constitute destructive effects directly leading to the deterioration of bilateral, regional or global relations, especially when the condition of state responsibility is not relevant. Yet, the subsequent societal, economic and political effects may transit national borders potentially threatening international peace and security, including stability and the continuity of friendly relations.

Path 3. Cyberterrorism destabilizes international and domestic relations

Cyber-attacks that meet the examined general criteria of terrorism take place within an on-going contestation, dispute or open conflict, potentially intensifying or widening the conflict over international borders. Rather than creating destructive or widely harmful effects, the attacks and the subsequent propaganda create fear, fertilize hate, and lead to question of the powers of local or national authorities. This may also lead to violations of human rights and democratic principles.

Path 4. Insecurity, injustice, and underdevelopment trigger cyberterrorism

Continued open or latent conflict or perceived insecurity, injustice and underdevelopment trigger cyberterrorism similarly as these factors facilitate crime, insurgency, and conventional terrorism. While in the previous paths the stimulus-response dynamic was horizontally built on cyberterrorist attacks, here the dynamic rests on an unjust or otherwise imbalanced vertical relationship. Wirtz (2017) notices how cyberterrorism may appear as an easy and cheap option to export politically motivated causes and extremist violence.

Policing and managing cyberterrorism

Terrorism (proper) has mainly been tackled by two approaches. During recent years, the most notable measures have included criminalizing different forms and facilitation of terrorism, following acts with punishment, and the projection of military force to exterminate terrorist and their base areas. The ‘Global War on Terrorism’ that the Bush administration launched after the September 11, 2001 attacks is the strongest manifestation of this widely shared approach.

A rather different approach focuses on the root causes of terrorism, in particular on peace, justice, and development but also on the facilitating issues, especially financing of terrorism. (UNCTC 2001; Hippel 2004, pp. 109, 113–115; Weimann, 2013) Both aspects are present in the 28 September Security Council Resolution 1373 (UNSC, 2001). The Security Council was determined to combat threats to international peace and security caused by terrorist acts by all means. Moreover, the resolution recognized states’ ‘right of individual or collective self-defence’ as legitimate responses to terrorism, thus logically applicable in case of cyberterrorist attacks with similar effects. The Security Council decided on measures *inter alia* to prevent and suppress the financing of terrorist acts, suppressing recruitment, and preventing movement of terrorists.

Measures to tackle cyberterrorism add three technologically oriented policy approaches to the toolbox: export controls to prevent proliferation of dual-use goods and technologies; the prevention of the use of ICTs for terrorist purposes; and the improvement of resilience of national information and other infrastructure.

Export controls – political and regulative measures to limit or prevent transfer of determined sensitive materials, goods or technologies to specified states or non-state actors, that cover advanced conventional, chemical, biological and nuclear armament and materials – function fairly well. In the field of ICTs, security, operational, and industrial interests make the borderlines between acceptable and unacceptable are more subjective and political.

The European Union (EP, 2018) has been revising its export control policy. It has noticed how cyber-surveillance technologies can be used in violation of human rights or international humanitarian law, or in a manner that poses a threat to international security. The EU wants to include five items into its control regime: mobile telecommunications interception equipment; intrusion software; monitoring centres; lawful interception systems and data-retention systems; and digital forensics. Similarly, the Wassenaar Arrangement (WA, 2017) targets within the categories of electronics, computers, telecommunications and ‘information security’, components, equipment, and software that can be employed for defeating, weakening or bypassing information security.

To target potential cyberterrorists, export controls need to cover capability elements that enable the design and employment of tools to penetrate, weaken or defeat information security systems and software. The US Commerce Control List (DOC, 2018) has such an approach. The Control List is organized into categories and product groups, the former containing, among others, electronics, computers, telecommunications, and information security. Most importantly, the List differentiates product groups into systems, test, inspection and production equipment, material, software, and technology targeting not only the current but also future technologies. The Australian Defence and Strategic Goods List (DOD, 2018) covers export, supply, publication and brokering of specified goods, software and technology, potentially also including advanced level teaching and applied or experimental research.

Behavioural-cognitive, technical, and normative measures have been taken mainly to limit terrorist propaganda and messaging over the Internet, improve societal and individual resistance against terrorist calls, and enhance legal capacity as well as international cooperation.

Following the Security Council Resolution 2354 (2017) and the UN Counter-Terrorism Committee ‘Comprehensive International Framework to Counter Terrorist Narratives’ (S/2017/375) the ICT for Peace Foundation launched a ‘Tech Against Terrorism’ project to foster multi-stakeholder cooperation in countering the terrorist use of ICTs. The project seeks to unite the technology industry, civil society, academia, and government to ‘disrupt terrorists’ ability to use the internet in furtherance of terrorist purposes’. It advocates an industry-led, self-regulatory approach focusing on terms of service and respect of rights, addressing harmful usage and content, and transparency reports, where the respect of human rights and fundamental freedoms function as an underlying principle (Tech against terrorism, 2018). Facebook, Google, Twitter, and Microsoft launched a parallel initiative – Global Internet Forum to Counter Terrorism – with a similar focus on disrupting terrorist use of (their) technological platforms for propagandist purposes (GIFCT, 2018).

The interest in counter-communication measures and techniques originates from the emergence of ‘Islamic State’ videos on home screens, laptops and smart phones. The violent images and the relatively successful recruitment triggered governments and corporation to take action. (Ferguson, 2016, pp. 9–15; Reed, Ingram and Whitaker, 2017, pp. 9–10) Several governments also want to control the flow and content of information within their jurisdiction and ‘national segment’ of cyberspace. Capabilities to monitor, collect, analyse, and interfere with communications do not differentiate their targets. They can be used also for

countering foreign influence operations, investigating cyber and other crimes as well as for political and suppressive purposes. Countering cyberterrorism is a useful, politicized and economically rewarding platform where civil liberties can easily be threatened – on-line and off-line (Weimann 2004 and 2013; ECJ 2014).

The methods employed range from strategic communication and counter-narratives to restricting content to closing websites and on-line services. For example, Facebook's guidelines to restrict harmful content clearly referred to terrorism by not allowing 'people or groups engaging in premeditated acts of violence to achieve a political, religious, or ideological aim to maintain a presence ... on our platform' (Facebook, 2018). The latest guidance does not single out the aims of acts but speaks of 'violent mission' or engagement 'in violence' (Facebook 2019). Twitter (2018), another platform for short, simple and populist messaging, allows 'some forms of graphic violence' but forbids such live videos and illegal content. Twitter also reserves a right to 'sometimes require you to remove excessively graphic violence'. On the other hand, social media platforms allowed the Christchurch March 2019 a terrorist manifesto and the actual terrorists act, the shooting of Muslim worshippers, being widely distributed. (WP, 2019)

Reed, Ingram and Whitaker (2017, pp. 39–43) recommend comprehensive and multi-platform disruption of violent extremist networks. The created vacuum is to be filled with clear, simple-to-understand messaging targeting motivational drivers. Perhaps most importantly, 'strategic communications', that is messages from the establishment, need to be synchronized with actions and events on the ground. Furthermore, well-meaning closing of websites and accounts may hinder intelligence gathering and other law enforcement operations.

For example, Germany (2017), Singapore (2019) and France (2019) have issued legislation to prohibit open incitement and so-called hate-speech. The German Act (*Netzwerkdurchsetzungsgesetz (NetzDG)*) requires social media sites to quickly remove hate speech, fake news, and illegal material (DB, 2017). The French Bill follows the German example of obliging social media platforms to remove hateful and violent content (*The Guardian*, 2019). The Singaporean 'Protection from Online Falsehoods and Manipulation Act' (POFMA) focuses on the prevention of 'false statements of fact' (SG, 2017: §5) a person communicates, which could among others 'incite feelings of enmity, hatred or ill-will between different groups of persons' as well as be prejudicial to security, public health or friendly relations or influence the outcomes of elections (§7b:i,ii,iii,iv,v). While focusing on peoples' communications, the Singapore legislation enables authorities to take measures 'to counteract the effects of such communication' (§5).

Disrupting the terrorist use of the Internet for propaganda and incitement purposes is a multifaceted issue. It is based on the assumption that propaganda works, that it gathers support for the desired political change. Most importantly, it assumes that terrorist, or 'violent extremist', messaging radicalizes youth to follow the (terrorist) cause. As communication is regarded as central to terrorism, denying and degrading that communication is believed to provide a solution. Ferguson (2016), however, points out that there is no established linkage between on-line exposure to propaganda and radicalization. Reed, Ingram and Whittaker (2017, pp. 11–12) acknowledge Ferguson's critique but, even after referring to the terrorists believing in the radicalizing effects of propaganda, notice that more research is needed to understand this relationship. In fact, Gross, Canetti and Vashdi (2017, p. 55) have shown how exposure to cyberterrorism increases public support for restrictive policies, for example Internet surveillance, strict government regulation of the Internet, and a forceful military response to cyberterrorism. Furthermore, they note that these attitudes may impinge upon the tolerance and confidence necessary for a vibrant and open democratic society. Not

surprisingly, the afore-mentioned three 'hate-speech acts' have been criticized as granting too wide powers to the governments and respective ministries and agencies, potentially leading to censorship and suppression of basic human rights.

Governments may want to disrupt Internet services for purposes other than counter-terrorism. Indeed, after the August 2019 mass shootings (murders) in El Paso and Dayton, President Trump blamed (among others) the Internet for providing 'a dangerous avenue to radicalize disturbed minds and perform demented acts' and called for the development of detection tools (Trump, 2019). As the fear of terrorism increases, lack of conceptual clarity, and evidence, may lead to politically or financially motivated labelling. In the wise words of Toni Morrison (1993) such '[R]uthless [language] in its policing duties ... has no desire or purpose other than maintaining the free range of its own narcotic narcissism, its own exclusivity and dominance'. Activists and hacktivists, cybercriminals and dissidents may find themselves becoming (cyber)terrorists; no algorithm or technical monitoring of Internet traffic or human and organizational behaviour is value free. Moreover, disrupting terrorists using the Internet to communicate their sermons and power, inevitably hinders law enforcement and national security authorities in collecting useful intelligence information.

Strengthening domestic societal, organizational or technological resilience does not require asking who the potential malicious actor is. Improved resilience, by default, reduces systemic and behavioural vulnerabilities. It helps to prevent possible attacks against, and deny disruptive and destructive effects in, critical infrastructure and industrial systems and essential societal services. Practically all national cyber or information security strategies pay keen attention to improving the protection of critical (national) infrastructure – with or without direct references to cyberterrorism (Kerttunen & Tikk, 2019). Similarly, international expert organizations dealing with vital and sensitive technologies and services – such as the International Atomic Energy Agency, the International Civil Aviation Organization, the International Maritime Organization, and the Transported Asset Protection Association – have issued guidelines and taken measures to improve sectorial cyber resiliency against accidents and incidents.

Deterrence by punishment, and imposing costs on an attributed attacker, are temporarily advocated approaches to also deal with cyberterrorism (Klein, 2015; US, 2018). Despite all the challenges of understandable communication and rational decision-making, deterrence may function among governments. Its value in projecting any 'healthy fear of God' on extremists can nevertheless be questioned. On the contrary, terrorism salutes harsh countermeasures. For some terrorists, the anticipated reward may be martyrdom, but for the terrorist cause the ultimate reward is heightened attention, abusive security measures and polarized societies, if not necessarily revolution, but a turn of the political tide.

Conclusion

Advanced information and communication technologies have created a distinct space for activities where states, organizations, groupings, and individuals seek to promote their causes. It is only logical that terrorists, terrorist messaging, and terrorist activities exercise influence in this area of opportunism.

That the cohorts of, for example, 'Islamic State' or Boko Haram may employ Cryptocat, Facebook, Hushmail, Kik, ProtonMail, RedPhone, Tails, Telegram, Threema, Tor, Twitter, Signal, SureSpot, WhatsApp, or Wickr – that is the latest catalogue of encrypted apps, browsers, chat tools, email services, operating systems and phone communications, and layman social platforms – does not make them terrorists. Governments, journalists, social

activists, and various informants utilize such hidden or anonymous services, too. Actors become regarded as terrorists because of their intention to pursue political influence through intimidation and violence. The act itself and its intended or caused effects count.

Cyberterrorism is but one method of terrorism. For the most advanced and ambitious groupings it may become one way to create destructive and terrorizing effects. For the less advanced, it may appear as a lucrative option.

Cyberterrorism is a conceptual construction. We have fortunately not yet witnessed death and physical destruction through digital means. Intimidating people and influencing opinion is as yet a reality beyond the usual accounting of *inter alia* recruitment, communication, and training. Therefore, we should not wait for death and destruction to occur before taking action. Most importantly, we should better acknowledge the public and political influence on-line terrorism has upon us.

Cyberterrorism can indirectly threaten international peace and security. By inciting hatred and harsh responses, it deteriorates bilateral relations, regional stability, and domestic peaceful conditions. It escalates in-built tensions and latent and on-going conflicts. When cyberterrorism is attributable to a foreign government, it is likely to threaten international peace and security without such conditioning public factors.

Measures to counter cyberterrorism are primarily designed to solve technical, societal, and national challenges. These measures indirectly strengthen international peace and security. Normative, organizational, and technical measures reduce vulnerabilities against several types of threat actors, vectors, and vulnerabilities, including unintentional incidents and insider threats.

As the UN Security Council (2014) has reaffirmed,

universal adherence to and implementation of the rule of law, as well as emphasis on the vital importance it attaches to promoting justice and the rule of law as an indispensable element for peaceful coexistence and the prevention of armed conflict.

Strengthening international peace and security, adherence to rule of law, respecting human rights and supporting sustainable development goals help to prevent and root out terrorism. Enhancing domestic resilience and improving incident management and forensic and attribution capabilities, prevents terrorism from achieving its destructive and transformative objectives and avoid false attribution, thus reducing the most probable causes of terrorism threatening international peace and security. Export controls created to prevent the acquisition of weapons of mass destruction and advanced conventional armament need to include ICT systems, equipment, and software but also capability elements that help design cybertools to penetrate, weaken or defeat governmental, corporate and individual information security.

Imposing intrusive restrictions and law enforcement measures may appear a good option for many governments. However, since terrorism tries to provoke the hardening of political and social attitudes, harsh measures should be applied with caution. Export controls can be seen as unjust and increase national insecurity. Terrorizing on-line messaging and incitement needs to be disrupted but mainly to prevent societal radicalization and a cycle of revenge.

The Baader-Meinhof/*Rote Armee Fraktion* was a group that tried to provoke the Federal Republic of Germany into class struggle and revolution in the 1970s. With the help and exploitation of social media, contemporary terrorists are far more successful in manipulating domestic and global attitudes – often harshly reactionary rather than supportive of terrorism. Extraordinary powers and non-transparent security measures degrade the liberal order and modern way of life that terrorists of all colour despise. By restricting our preferred way of

life, and by limiting individual freedoms, we are polarizing our societies. We are also fostering a world order of difference and intolerance, a world order of fear and hatred, where international peace and security easily becomes exposed, vulnerable, and breached.

References

- Australian Government Department of Defence (DOD) 2018 Australian Export Controls and ICT. Available from: www.defence.gov.au/ExportControls/ICT.asp [accessed 7 November 2018].
- Boulden, J. & Weiss, T.G. (eds) (2004) *Terrorism and the UN. Before and After September 2001*. Bloomington, Indiana University Press.
- BRICS (2015) VII BRICS Summit Ufa Declaration. Available from: <http://en.brics2015.ru/documents/> [accessed 9 February 2018].
- Buzan, B. (1983) *People, States and Fear*. Brighton, Harvester Wheatsheaf.
- Coats, D.R. (2018) Worldwide threat assessment of the US intelligence community. Available from: www.dni.gov/index.php/newsroom/congressional-testimonies/item/1845-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community [accessed 14 February 2018].
- Conway, M. (2005) The Media and cyberterrorism: A study in the construction of 'reality'. Available from <http://azumisan.asuscomm.com/Free%20E-Books/Cyber%20Security/The%20Media%20And%20Cyberterrorism%20-%20A%20Study%20In%20e%20Construction%20Of%20e%20%80%98Reality%20%80%99.pdf> [accessed 20 September 2018].
- Court of Justice of the European Union (ECJ) (2014) Judgment in Joined Cases C-293/12 and C-594/12. Digital Rights Ireland and Seitlinger and Others.
- Denning, D.E. (2000) Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. Available from: <https://stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf> [accessed 15 February 2018].
- Department of Commerce (DOC) (2018) Commerce control list. Available from: www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl [accessed 7 November 2018].
- Department of Information and Communication Technology (DICT) (2017) *National Cybersecurity Plan 2022*. Manila.
- Deutscher Bundestag (2017) Bundestag beschließt Gesetz gegen strafbare Inhalte im Internet. Available from: www.bundestag.de/dokumente/textarchiv/2017/kw26-de-netzwerkdurchsetzungsgesetz-513398 [accessed 12 July 2019].
- Dunn Cavelty, M. (2008) Cyber-terror – looming threat or phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology & Politics*. 4(1): 19–36.
- Eriksson, J. (2001) Cyberplagues, IT, and security: Threat politics in the information age. *Journal of Contingencies and Crisis Management*. 9(4): 211–222.
- European Parliament (EP) 2018. Review of dual-use export controls. Available from: [www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI\(2016\)589832](http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)589832) [accessed 6 November 2018].
- Facebook (2018) Community Standards, I, 2. Available from: www.facebook.com/communitystandards/violence_criminal_behavior/dangerous_individuals_organizations/ [accessed 25 April 2018].
- Facebook (2019) Community Standards, I, 2. Available from: www.facebook.com/communitystandards/dangerous_individuals_organizations/ [accessed 20 May 2018].
- Ferguson, K. (2016) Countering violent extremism through media and communication strategies. A review of the evidence. *Partnership for Conflict, Crime and Security Research* (March 1).
- Fischer, G. (1967) Sociology. Fischer, G., De George, R.T., Graham, L. & Levine, H.S. *Science and Ideology in Soviet Society*. New York, NY, Atherton Press, pp. 1–46.
- French Prime Minister (2015) *French National Digital Security Strategy*. Paris.
- Global Internet Forum to Counter Terrorism (2018). Available from <https://gifct.org/> [accessed 20 September 2018].
- Gross, M.L., Canetti, D., & Vashdi, D.R. (2017) Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity*. 3(1): 49–58.
- Group of Seven (G7) (2017) Taormina Statement on the Fight Against Terrorism and Violent Extremism. Available from: www.g7italy.it/sites/default/files/documents/G7%20Taormina%20Statement%20on%20e%20Fight%20Against%20Terrorism%20and%20Violent%20Extremism_0.pdf [accessed 9 February 2018].

- Group of Twenty (G20) (2017) G20 Action Plan on Countering Terrorism. Available from: <https://eu-un.europa.eu/g20-leaders-statement-countering-terrorism/> [accessed 9 February 2018].
- The Guardian (2018) Facebook accused of censorship after hundreds of US political pages purged. Available from: www.theguardian.com/technology/2018/oct/16/facebook-political-activism-pages-inauthentic-behavior-censorship [accessed 26 October 2018].
- The Guardian (2019) France online hate speech law to force social media sites to act quickly. Available from: www.theguardian.com/world/2019/jul/09/france-online-hate-speech-law-social-media [accessed 12 July 2019].
- Her Majesty's Government (HMG) (2000) *Terrorism Act 2000*. Available from: www.legislation.gov.uk/ukpga/2000/11/contents [accessed 12 February 2018].
- Her Majesty's Government (HMG) (2016) *National Cyber Security Strategy 2016–2021*. London.
- Hippel, K. von (2004) Improving the international response to transnational terrorist threat. In Boulden, J. & Weiss, T.G. (eds), *Terrorism and the UN. Before and After September 2001*. Bloomington, Indiana University Press.
- Jarvis, L., Macdonald, S., & Nouri, L. (2014) The cyberterrorism threat: Findings from a survey of researchers. *Studies in Conflict & Terrorism*. 37(1): 68–90.
- Jarvis, L., Macdonald, S., & Whiting, A. (2017) Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat. *European Journal of International Security*. 2(1): 64–87.
- Kerttunen, M. & Tikk, E. (2019) Strategically normative. Norms and principles in national cybersecurity strategies. EU Institute for Security Studies. Available from: https://eucyberdirect.eu/content_research/a-normative-analysis-of-national-cybersecurity-strategies/ [accessed 10 May 2019].
- Klein, J. (2015) Deterring and dissuading cyberterrorism. *Journal of Strategic Security*. 8(4): 23–38
- Lewis, J. (2002) Assessing the risks of cyberterrorism, cyber war, and other cyber threats. Washington, DC, Center for Strategic and International Studies.
- Macdonald, S. (2015) Cyberterrorism and enemy criminal law. In Ohlin, J.D., Govern, K., & Finkelstein, C. (eds) *Cyberwar. Law and Ethics for Virtual Conflicts*. Oxford, Oxford University Press, pp. 57–75.
- Morrison, T. (1993) Nobel Lecture (December 7). Available from: www.nobelprize.org/prizes/literature/1993/morrison/lecture/ [accessed 9 August 2018].
- The Ministry for Foreign Affairs of the Russian Federation (RU MFA) (2016) *Doctrine of Information Security of the Russian Federation*. Available from: www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptlCk6BZ29/content/id/2563163 [accessed 26 October 2018].
- Parliament of Singapore (SG) (2019) *Protection from Online Falsehoods and Manipulation Bill*. Available from: www.parliament.gov.sg/docs/default-source/default-document-library/protection-from-online-falsehoods-and-manipulation-bill10-2019.pdf [accessed 12 July 2019].
- Reed, A., Ingram, H.J., & Whittaker, J. (2017) Countering terrorist narratives. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs (November).
- Riglietti, G. (2016) Defining the threat: What cyber terrorism means today and what it could mean tomorrow. *The Business and Management Review*. 8(3): 12–19.
- Serna Galvan, M.L. de la (2011) Interpretation of article 39 of the UN Charter (Threat to the peace) by the Security Council. *Anuario Mexicano de Derecho Internacional*, XI, 147–185.
- Siemens (2018) Charter of Trust. Available from: www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/cybersecurity-charter-of-trust.html [accessed 17 February 2018].
- Sinclair S.J. & Antonius D. (2013) *The Political Psychology of Terrorism Fears*. Oxford, Oxford University Press.
- Smith, B. (2017) The Need for a Digital Geneva Convention. *RSA Conference*. Available from: <https://mscorpmedia.azureedge.net/mscorpmedia/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf> [accessed 2 February 2018].
- Tech against terrorism (2018). Available from www.techagaintsterrorism.org/ [accessed 20 September 2018].
- Thomas, D. (2002) Cyberterrorism: Is the nation's critical infrastructure adequately protected? Hearing before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental relations. Available from: www.scribd.com/document/341380889/house-hearing-107-congress-cyberterrorism-is-the-nation-s-critical-infrastructure-adequately-protected [accessed 26 October 2018].

- Tikk, E. & Nagelhus Schia, N. (2020) High road or the back seat? The role of the UN Security Council in cybersecurity. In Tikk, E. & Kerttunen, M. *Routledge Handbook of International Cybersecurity*. Abingdon, Routledge.
- Trump, D. (2019) Prepared remarks (5 August). Available from: www.washingtonpost.com/politics/2019/08/05/where-blame-weekends-mass-shooting-lies-according-trump/ [accessed 8 August 2019].
- Twitter (2018) The Twitter Rules. Available from: <https://help.twitter.com/en/rules-and-policies/twitter-rules> [accessed 29 October 2018].
- United Nations Department of Political Affairs (DPA) (2018) Security Council Practices and Charter Research Branch. *Repertoire of the Practice of the Security Council*. Available from: www.un.org/en/sc/repertoire/structure.shtml [accessed 11 February 2018].
- United Nations General Assembly (UNGA) (1994) Measures to eliminate international terrorism. A/RES/49/60.
- United Nations General Assembly (UNGA) (2006) The United Nations Global Counter-Terrorism Strategy. A/RES/60/288.
- United Nations Group of Governmental Experts (GGE) (2010) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/65/201.
- United Nations Group of Governmental Experts (GGE) (2013) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/68/98.
- United Nations Group of Governmental Experts (GGE) (2015) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174.
- United Nations Office on Drugs and Crime (UNODC) (2012) *Use of Internet for Terrorist Purposes*. New York, United Nations.
- United Nations Security Council (UNSC) Resolutions no. 688 (1991); 731 (1992); 841 (1993); 1132 (1997); 1269 (1999); 1368 (2001); 1373 (2001); 2341 (2017a); and 2395 (2017b).
- United Nations Security Council (UNSC) (2014) Statement by the President of the Security Council. S/PRTS/2014/5.
- United Nations Security Council Counter-Terrorism Committee (2001) Resolution 1373. Directory of International Best Practices, Codes and Standards. Available from: www.un.org/sc/ctc/resources/databases/recommended-international-practices-codes-and-standards/united-nations-security-council-resolution-1373-2001/ [accessed 1 November 2018].
- United Nations Security Council Counter-Terrorism Committee (2018) International Legal Instruments. Available from: www.un.org/sc/ctc/resources/international-legal-instruments/ [accessed 2 February 2018].
- United States (US) (2011) *International Strategy for Cyberspace*, Washington, DC, The White House.
- United States (US) (2018) *National Cyber Strategy of the United States of America*, Washington, DC, The White House.
- Värk, R. (2009) Terrorism as a threat to peace. *Juridica International*. XVI: 216–223.
- Washington Post* (WP) (2019) The New Zealand shooting shows how YouTube and Facebook spread hate and violent images – yet again. (15 March).
- The Wassenaar Arrangement Secretariat (2017) Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.
- Weimann, G. (2004) *Cyberterrorism. How Real Is the Threat?* United States Institute of Peace. Report no. 119.
- Weimann, G. (2006) *Terror on the Internet*. Washington, DC, USIP Press Book.
- Weimann, G. (2013) *Terrorism in Cyberspace. The Next Generation*. New York, Columbia University Press.
- Wirtz, J.J. (2017) The Cyber Pearl Harbor. *Intelligence and National Security*. 32(6): 758–767.
- Yunos, Z., Ahmad, R., & Yusoff, M. (2014) Grounding the component of cyber terrorism framework using the grounded theory. *Science and Information Conference*. 523–529.

INFORMATION OPERATIONS

Jouni Flyktman, Aki-Mauri Huhtinen and Lars Koreman

In this chapter we investigate information operations (IO) as a part of international peace and security. In contrast to cyber operations, the focus in information operations is on influencing human decision-making, attitudes, and behaviour. The chapter is motivated by the current discussion on information operations in the scientific community and in the media. Many of the books on this subject focus on analysing the doctrine of information operations (Allen, 2007; Armistead, 2004; Armistead, 2007; Armistead, 2010; Paul, 2008; Steele, 2006). As the term information warfare has tended to be used interchangeably with the term information operations, similar content can be found in books on information warfare (Jones & Kovacich, 2016). Compared to the abundance of doctrine-based writing, public analyses of the practice of information operations are rare, however (Larson et al., 2009; Muñoz, 2012). After the Russian occupation of Crimea, there was a surge in literature on Russian information operations (NATO Strategic Communications Centre of Excellence, 2004; 2015a; 2015b; 2016a; 2016b; 2016c; Pynnöniemi & Rácz, 2016). Yet despite numerous publications on the subject, attempts to develop a theory of information operations have been scarce (Armistead, 2010). The lack of theory is, however, only a partial shortcoming since there is a well-established body of propaganda theories that has been updated to cover modern information technology (Jowett & O'Donnell, 2012).

The concept of information operations has been used quite loosely and applied rather generally to refer to a wide variety of activities. Despite the abundant literature emphasising the importance or threat of information operations, perceptions of the significance or usefulness of IO as a military or foreign policy tool are divided. Hence, this chapter addresses two fundamental questions about the subject: 1) What are information operations? and 2) What is the significance of information operations in the area of international peace and security?

In order to answer the first question on the definition and meaning of information operations, we will carry out a conceptual analysis of the term. In addressing the second question on the significance of information operations, we will limit our analysis to the contexts of international relations and warfare or military operations. These contexts were chosen as the most relevant for the purposes of this book, even though information operations could exist in other contexts as well. The analysis of the significance is guided by the ideas presented in the Introduction to this book inasmuch as we investigate information operations primarily as

an international or a cross-border activity, and the way in which such operations can impact international peace and security.

The analysis is based, on the one hand, on the existing literature on information operations and warfare and, on the other, on publicly available doctrine and policy documents, since the latter are the most relevant readily available sources. In order to analyse the significance of IO, we have developed a theoretical framework for the analysis, based on theories of international relations, the social construction of reality, and the philosophy of information.

Defining information operations

In both common parlance and scientific discourse, the term information operations has been used to refer to a wide range of activities. Typical activities pertaining to IO in the literature include exploiting falsified information or disinformation (Pomeratsev, 2015), the use of computer networks to create desired effects (Ventre, 2009), attempts to affect perceptions or behaviour, and attempts to influence the adversary's decision-making (Allen, 2007). There has also been a tendency for the expression to be used interchangeably with the terms information warfare, information activities and information campaigns.

The meaning of the concept has evolved in line with the evolving conception of warfare. Initially in the 1990s, information warfare signified the action on the digital battlefield supported by the latest information technology such as precision-guided weapons and real-time situational awareness systems, or actions taken to achieve information superiority over the adversary (United States Joint Staff, 1996, p. GL-8). At the beginning of the 2000s, the term was often used to refer to the use of computer networks to create desired effects, also better known as cyber warfare. Currently, the term refers most often to influence activities or, more traditionally, to propaganda.

One of the underlying factors behind the changing conception of warfare has been the development of technology. The growing significance of information technology in the armed forces during the revolution in military affairs (RMA) in the United States resulted in designating the new form of warfare 'command and control warfare', in which so-called information superiority was seen as a key element (Arquilla, 1994, p. 24). Subsequently, the term information warfare has been used interchangeably with command and control warfare. Both terms are rather problematic upon closer inspection. Information technology, namely sensors and the real-time distribution of information, has unquestionably changed warfare. However, information and its exploitation have always been essential constituents of success in warfare. Hence, if the defining characteristic of information warfare was the exploitation of information, all warfare would have to be referred to as information warfare.

Information operations in the form of influencing have been shaped by the evolution of information technology. New technology has enabled huge audiences to be reached worldwide with low-cost solutions, while the exploitation of big data has made it possible to tailor messages for small groups and even for individuals. This aligns with two theoretical notions of propaganda. First, the channel for conveying information operation messages is selected based on the target's ability to receive messages and not on the ability to transmit. Second, propaganda is most effective when it is based on the prejudices of the target audience (Jowett & O'Donnell, 2012). For this reason, the more familiar the propagandist is with the prejudices of the target audiences, the more effectively the propaganda can be tailored to those audiences. A concrete example of this kind of tailored influence was presidential candidate Donald Trump's election campaign in 2016, in which social media data was exploited in tailoring effective messages.

The current definition of information operations in the US military doctrine is

the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.

(United States Joint Staff, 2014)

According to this definition, the aim is to affect decision-making and the target is the adversary or potential adversary. The method employed can be any of the so-called information-related capabilities which, in turn, are defined as the tools, techniques, or activities that affect any of the three dimensions of the information environment (United States Joint Staff, 2014).

In the NATO doctrine, information operations are defined as

a staff function that analyses, plans, assesses and integrates information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and North Atlantic Council (NAC) approved audiences in support of Alliance mission objectives.

(United Kingdom Ministry of Defence, 2014)

This definition is very similar to the US definition, although the scope is wider since, in addition to affecting will, which is close to decision making, the goal is also to affect understanding and capability. Similarly to the US definition, any methods can be employed to achieve these aims. The target audience of the NATO definition is wider since NAC-approved audiences could in principle include any audiences.

These doctrine definitions situate information operations solely in the context of military operations, but for the purposes of analysing information operations as an international security phenomenon, we cannot adopt such a limited definition.

A concept closely related to information operations is that of psychological operations. In the US doctrine, psychological operations were renamed military information support operations, or MISO, for a short period of time, apparently to diminish the negative connotations of the term psychological operations. The latter are one of the information-related capabilities that can be used in information operations. Despite the doctrinal separation of the concepts, the term psychological operations is often used interchangeably with information operations in practice. Psychological operations are defined as

planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behaviour of foreign governments, organizations, groups, and individuals in a manner favourable to the originator's objectives.

(United States Joint Staff, 2011)

This definition closely resembles one of the classic definitions of propaganda:

the deliberate and systematic attempts to shape perception, manipulate cognitions and direct behaviour to achieve a response that furthers the desired intent of the propagandist.

(Jowett & O'Donnell, 2012)

In both of the definitions, the intention is to affect perceptions and behaviour to further one's own interests. The methods are not defining characteristics of propaganda. Instead, in propaganda all available methods are deployed in an innovative manner.

In the Western doctrines, psychological operations and public affairs are strictly separated. The separation, however, seems artificial if it is assessed functionally and from the recipient's point of view. Functionally, both public affairs and psychological operations are employed to support the military operation. They both operate in the cognitive domain where the decision-making takes place. Processually, they are similar since both require target audience analysis, planning and tailoring the message in order to be effective. The usual rationale for the separation is maintaining the credibility of public affairs. However, credibility is a prerequisite for any effective communication effort. A military operation and its information activities are assessed as a whole by outside recipients and any loss of credibility due to IO will affect the credibility of public affairs, even if the military operation itself were able to differentiate between these functions.

Since this is a handbook of *cybersecurity*, the relationship between the concepts *information operation* and *cyber operations* deserves special attention here. The main difference between the concepts is that cyber operations are method-driven whereas information operations are purpose-driven. Cyber operations refer to actions conveyed in or via cyberspace. Information operations, on the other hand, are defined by the objective of affecting decision-making or opinion. This conceptual relationship has only been explicit in the US military doctrine since 2013 (United States Joint Staff, 2013, p. I-5). In the light of this conceptual relationship, the two concepts effectively intersect: information operations are realized by cyber operations. An example of the intersection is the alleged Russian influence on the US presidential elections in 2016, in which cyber methods were deployed to collect the information needed in the information operations against Democratic candidate Hillary Clinton.

Disinformation is often associated with information operations, with the connection between disinformation and propaganda being thoroughly discussed in the literature on the latter. Even if the common perception of propaganda often assumes that it is based on lies, disinformation is not a defining characteristic of propaganda. Indeed, disinformation is often avoided in propaganda in order to preserve its credibility. Following the established relationship between disinformation and propaganda, we exclude disinformation as a defining characteristic of our definition of information operations, even if it may be regarded as a method in the process.

A usual claim in the literature on information operations is that the Russian conception of IO is more comprehensive than the Western conception because it includes both information-psychological and information-technical aspects. Allegedly, the psychological aspect is more important in Russia than in the West, and there are a number of factors contributing to this difference. For example, Russia has lagged behind the United States by approximately ten years in terms of computerization (International Telecommunication Union, 2015, p. 46), with the result that technological vulnerabilities have been less significant as a national security threat. The difference can also be explained by the dissimilarities in political cultures. Upon closer examination, information-psychological operations correspond with our definition of information operations, while information-technological operations correspond to cyber operations.

Given the preceding conceptual analysis, we define information operations as deliberate activities designed to affect the attitudes, behaviour and decision-making of selected audiences, such as political or military leadership or larger populations, in order to further the interests of the originator. The means and methods may vary since they are not the defining

characteristics of information operations. Cyber operations and disinformation are excluded from the definition but they can be deployed as methods. Our definition intentionally differs from the doctrine definitions given by the US and NATO in order not to confine our study to the context of military operations.

Information operations in international relations

In the light of our definition of information operations, we now turn to examine the role of IO in international relations. The basic unit of analysis in international relations is the nation–state and in our discussion we focus on information operations as a part of the foreign policy of nation–states.

Attempts to build a theory of information operations in the literature are based on the claim that information is the most important element of power (Armistead, 2004; Armistead, 2010). Power is one of the central concepts in international relations and thus we have to explore the relationship between power and information operations. Power in international relations cannot be based on formal *authority* because there are no formal relationships of authority in the international system, and therefore the power between states mainly entails *influence* (Brown & Ainley, 2005, p. 80).

Power is a central concept in the realist school of thought. Armistead (2010) notes that realists do not typically include information as a constituent of national power. Instead, they emphasize material forces and resources as a source of power. Morgenthau (1967), for example, defined sources of national power as natural resources, industrial production, military power, population, national character and morale, and the quality of diplomacy and government. In contrast, the informational element is defined as one of the elements of national power according to the DIME (diplomatic, information, military, economic) mnemonic in the National Security Strategy of the United States (2015). This fourfold division dates back to the 1950s at least when Lasswell identified information as one of the four policy instruments in addition to diplomacy, economics and force (Lasswell, 1958, p. 204).

The national security strategies of the United States and the security doctrines of the Russian Federation employ the language of realism when addressing information security. For example, the information security doctrine of the Russian Federation defines national interests in the information sphere. The interests are quite comprehensive ranging from critical infrastructure protection to information support for foreign policy, and the protection of traditional moral values (Доктрина информационной безопасности Российской Федерации, 2016).

Due to its emphasis on material factors, realism is not an adequate paradigm for explaining information operations in international relations. The basic logic in the theory tradition of constructivism is that the decisions and actions of states are explained by identities and interests that are determined in intersubjective social interaction (Weber, 2005). This logic makes constructivism highly appropriate for understanding information operations in international relations. According to the constructivist view, power is produced in social interaction between actors. States compete over their identities and the power balance between them is reflected in the discourse. Powerful states are able to dominate the discourse and shape the social reality. Challenging the status quo requires challenging the predominant discourse on international relations. A recent example has concerned Russia's challenge towards the Western conception of international security and the world order, which Russia regards as being dominated by Western states. This has manifested as a discursive competition regarding the great power status of the Russian Federation. The United States has

defined Russia a regional power that acts out of weakness (*Washington Post*, 2014). In contrast, in the Russian media Russia has been described as a geopolitical pole of the international system, with the military operation in Syria being cited as proof of the great power status of Russia (*Известия*, 2015).

As institutions and phenomena are socially constructed, information operations can be seen as a social construct. A substantial amount of the literature on information operations has been devoted to depicting IO as a threat to national security, with the threat duly being seen as socially constructed. Relatedly, representing information operations as a threat to national security can be seen as an act of securitization, in which a certain phenomenon is claimed to pose an existential threat to a referent object and extraordinary countermeasures outside of the normal political process are proposed to counter the threat (Buzan, Wæver & de Wilde, 1998). When securitizing information operations, the referent object is typically a nation– state, society, or Western values.

Liberalism as a school of thought might be relevant when analysing initiatives taken to establish international treaties to govern information operations or information warfare. Creating an international system of information security is one of the main objectives of the Russian information policy (*Доктрина информационной безопасности Российской Федерации*, 2016; *Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года*, 2013). However, the fuzzy line between political struggle and information operations might render attempts to define the scope of the treaty impossible. Another problem concerning treaties is that technology advances quickly and new ways to circumvent possible treaties might emerge at a faster pace than the treaties can be updated. Instead of treaties on information operations that are hard to achieve, more comprehensive measures to reduce tensions and build trust might be more effective. A possible solution could also be stricter regulation of social media companies to restrict information operations. In the European Union, stricter regulation of companies has already been proposed (Meserole & Polyakova, 2018).

Some theories of international relations, such as neoclassical realism, acknowledge the role of internal affairs of states in international relations. Internal affairs are important for understanding information operations for various reasons. First, information operations are more efficient when directed towards one's own population. Second, in authoritarian regimes, the government often attempts to monopolize the truth because the existence of different opinions accelerates unwanted political and social change. Typical means of monopolizing the truth include limiting the sources of independent information and harnessing the media to disseminate pro-government messages. A well-known example is the tight media control in the Russian Federation. Control over the media and the so-called information support of the media for foreign policy have been strategic aims in the Information Security Doctrine since 2000 and continued to be mentioned in the 2016 version (*Доктрина информационной безопасности Российской Федерации*, 2000 & 2016). According to many Western commentators, although control over the media in Russia is already high, it is expected to be tightened even further. A similar tendency has recently been observed in the United States where the Trump administration has tried to centralize and control public opinion by stigmatizing differing views as 'fake news'. Despite the misuse of the term by the Trump administration, fake news is actually a common technique in information operations. As the news media is instrumental in shaping public opinion, it is an important channel for the dissemination of propaganda (Zollmann, 2017).

A recent example of information operations in international relations was the alleged Russian interference in the US presidential elections in 2016. The influence operation was

claimed to be multifaceted in that multiple methods were employed (the Office of the Director of National Intelligence, 2017). Cyber methods were used to collect compromising information on the Democratic Party and that information was leaked to harm Hillary Clinton's campaign. The operation was supported by public propaganda (House Permanent Select Committee on Intelligence, 2018). The ability to affect the outcomes of elections is a powerful foreign policy tool, the effectiveness of which is based on the fact that it exploits the vulnerability of democracy itself instead of the technical vulnerabilities of voting systems. Manipulating actual votes is unnecessary if public opinion can be shaped with IO.

Many of the examples provided in this section underline the fuzzy distinction between information operations and normal and easily tolerable political influence. It is not possible to entirely separate the two. For conceptual clarity, we point out that in the military doctrines of the United States and NATO, the activities described in this section are typically referred to as strategic communication. Our wider definition of information operations corresponds with the scientific discourse on the topic and has accommodated treatment of the subject in the context of international relations.

Information operations in warfare

The second context for analysing the significance of information operations is warfare. Warfare itself is a multi-faceted phenomenon and concept. We approach it as the use of military capabilities to either coerce adversaries into, or deter them from doing something. The conception of war has evolved over centuries. Since the end of the Cold War, the predominant conception in the West has shifted from a clash of superpowers to expeditionary military operations. In Russia, in contrast, the geopolitical struggle between great powers is still the prevailing conception. The respective conception of war defines the role and characteristics of information operations in warfare. Most of the Western doctrine development has been devoted to information operations in expeditionary military operations because that has been the main contemporary conception of war in the West.

According to our definition in the context of warfare, information operations can take two possible forms, on the one hand affecting the adversary's military decision-makers, and affecting the perceptions and behaviour of populations or groups, on the other. In this section, we study both of these forms. The current US doctrine definition of information operations corresponds almost directly to the first meaning of our definition. The exact wording of the definition depicts information operations as a line of operation, the aim of which is to affect the adversary's decision-making (United States Joint Staff, 2014, p. GL-3). Seeing affecting the adversary's decisions as a line of operation puts it in a superimposed and supporting role in the military operation, even though the overall aim of the operation should be to affect the adversary's decision-making. The perceived need for a separate function to affect the adversary's decision-making can be seen as a symptom of separation from the very nature of warfare.

Affecting decision-making requires detailed and comprehensive knowledge about the adversary's information-gathering system, decision-making processes, and beliefs. For example, in order to deceive the adversary, coherent deceptive information must be fed to multiple intelligence and other channels. Deceptive information in one channel is easily ruled out by the adversary if it cannot be corroborated elsewhere (Clark & Mitchell, 2019, p. 99). In the case of deception, the deceptive information has to be congruent with the predispositions of the adversary in order not to be rejected. Similarly to deception, any other type of information operations to alter decision-making require feeding information to the

relevant reception channels of the adversary. This makes information operations inherently multi-faceted. Even if the entire aim of information operations is, by definition, to affect decision-making, very few studies on the subject take into account the decision-making processes of the adversary. One of the few analyses has been presented by Waltz (2007, p. 96).

Exploitation of the adversary's predispositions in order to affect decision-making is a central idea in the Russian reflexive control theory. According to the theory, specifically tailored information conveyed to the adversary would make the latter voluntarily choose courses of action beneficial to the exerciser of the reflexive control (Thomas, 2004). Conceptually, Russian reflexive control is therefore close to information operations in terms of affecting decision-making.

In military coercion, information operations could be employed to alter the cost-benefit analysis of the adversary. According to the theoretical model of military coercion, coercive success occurs when the expected potential costs of resistance outweigh the expected benefits (Pape, 1996, p. 16). By altering the perceived costs and the probability of suffering them, the adversary can be coerced to the will of the coercer. Information operations can be used as an effective deterrent to armed conflict if used proactively in the early phases of the conflict (Clark, 2010). The logic here is that by threatening the adversary with overwhelming military power, the adversary can be deterred from taking military action. Although this kind of threatening with military force does not necessarily constitute an information operation, the threat has to be supported by information operations or communications in order to be effective. Similarly, a show of force has to be accompanied by information operations or communications to even be recognized as a show of force. For example, the Russian cruise missile attack launched to Syria from the Caspian Sea was advertised as proof of the successful modernization of the Russian Armed Forces and as a sign of the great power status of Russia (*Известия* 2016).

In addition to deterrence, information operations can be employed to start a war or military operation. This could be done, for example, by provoking the adversary to take military action so that the adversary is perceived as the aggressor. This corresponds with the second meaning of information operations, namely influencing audiences to gain support for military operations. The aims of these operations depend on the target audience. When directed towards one's own population, the aim is to create public support for war. This is essential in expeditionary warfare since the benefits and the necessity are far less obvious than in homeland defence.

The most prominent functions in information operations supporting military operations entail arguing the benefits of the operations, on the one hand, and demonstrating their legitimacy, on the other. Recent examples include the Russian operations in Crimea and in Syria. The pattern of demonstrating legitimacy was similar in both operations in that Russia claimed to be acting at the request of the official government of Ukraine or Syria. In both cases, it was highlighted that the Federation Council gave the president permission to use armed forces outside the area of the Russian Federation. In order to emphasize the legitimacy of these actions, the actions taken by Western countries, and the United States in particular, were used as a point of comparison and heavily delegitimized as violations of international justice.

The use of military force needs to be justified by legitimizing the targets of kinetic action. In other words, taking people's lives calls for strong arguments. In recent expeditionary operations, the targets have been justified by appealing to the argument of fighting terrorism. Russia has used the same argument in the operation in Syria, making it hard for the West to categorically deny Russia's right to fight terrorism. Instead, the discursive struggle has

focused on defining just who the terrorists are. The identities of other actors besides the targets were also constructed. For example, Russia itself was represented as a helper in both operations and as a resolver of international security challenges in the Syrian operation. This is very similar to the Western approach in which interventions have been legitimized by helping civilians and resolving international security problems.

Western experiences of information operations have accumulated recently, for example in the US-led operation in Afghanistan. A study by Muñoz (2012) indicates that the results of information operations have been mixed in Afghanistan. Another study suggests that the most effective form of information operations is long-term face-to-face interaction between military commanders and the local populace, based on deep cultural understanding (Larson et al., 2009, p. 18).

Discussion and conclusions

This chapter has investigated the defining characteristics of information operations and their significance in international relations and warfare. We defined information operations as affecting the decision-making of the adversary and the attitudes and behaviour of different target audiences in order to further the interests of the originator. The definition turned out to be fuzzy with respect to normal political influence. This is a common feature among the doctrine definitions and the classical definition of propaganda. Our analysis showed, consistent with the introduction to this handbook, that the fuzziness is not caused primarily by ontological or epistemological factors, but by political ones. The actions are often called information operations or information warfare if conducted by the adversary, even if similar actions conducted by oneself are called communications or political influence.

The preceding observation is reflected in the perception of the significance of the information operations. In the national security strategies, information operations, or information warfare, are seen primarily as a threat to national security, and as a foreign policy tool for advancing one's own interests second. Military doctrines, however, describe information operations as an important tool in military operations.

The practical significance of information operations cannot be evaluated by doctrine and strategies alone. In order to prove the significance in practice, one needs to show a measurable change in decision-making, attitudes or behaviour, and also that the change was caused by something called information operations. In practice, the significance of information operations has been evidenced by recent military operations in which the mobilization of a country's own population has played an important part. Despite their significance, information operations do not usually provide any quick wins or fire-and-forget solutions. Instead, in practice, they are long-term efforts and are analogous to attrition or even trench warfare rather than manoeuvre warfare. Additionally, information operations seem to be most effective when directed towards one's own populations. The fact that Russia had to carry out military interventions in Crimea and Syria actually shows that information operations alone were insufficient foreign policy tools in international relations.

Information operations can exert effects on international peace and security. According to constructivist theory, the practices in international relations are socially constructed. Hence, using information operations as a foreign policy tool makes such operations more tolerable. Similarly, using disinformation in information operations can create a culture of mendacity in international relations. The effect of information operations on stability is mixed. They can either increase or reduce national, regional and global stability as they can

be used, on the one hand, to create tensions and divisions, and to promote the unity of social groups, on the other.

The discourse of information operations and information warfare – as well as ‘cyber war’ – has been seen to erode the line between war and peace. However, if we take the use of destructive violence in the form of military force as one of the defining characteristics of warfare, the sole application of information operations is distinct from warfare. There are certainly procedural differences for starting an information operation and starting a war. War without tensions and tense rhetoric would be an anomaly.

As a mitigating measure, countering disinformation with truthful information is typically recommended. However, the approach turns out to be problematic since absolute truths seldom exist in politics. Instead, a more effective mitigation measure could be engaging in dialogue and rationalizing one’s own views. Of course, this is useless if the adversary’s aim is not to discuss but to create chaos.

Recommendations for developing the doctrine of information operations exist in the literature since a large part of the latter is based on doctrine as the main source. Our addition to the recommendations entails placing the aims of information operations, namely affecting the will and decision-making of the adversary, at the centre of the operational art instead of superimposing information operations onto military operations as a separate line of operations.

Information operations still present numerous avenues for both theoretical and empirical research. Theoretical studies are needed to create a common theoretical foundation for the discipline. Empirical studies conducted thus far have mainly focused on the façade of information operations, namely its appearance in the media, and on the themes and discourses associated with it. Further empirical studies are needed on the processes and internal workings of information operations. The actual results achieved by information operations – changes in attitude, behaviour or decision-making – would also be research-worthy, even if the availability of relevant sources hindered any such empirical public domain studies.

The future of information operations will be inextricably intertwined with technological development. Technological advances and the adoption of artificial intelligence systems will change military decision-making. This will serve to enhance the decision-making process, but will also create new opportunities for information operations to affect decision-making. New vulnerabilities will emerge between those that are purely technological and those that are purely human. It has been predicted that more-than-human geopolitics will be the way to understand international security (Shaw, 2017). With these developments in mind, further research will be needed to advance understanding of the influence of new technology on information operations.

References

- Allen, P.D. (2007) *Information Operations Planning*. Boston, Artech House.
- Armistead, E.L. (ed.) (2004) *Information Operations: Warfare and the Hard Reality of Soft Power*. Washington, DC, Potomac Books.
- Armistead, E.L. (ed.) (2007) *Information Warfare: Separating Hype from Reality*. Washington, DC, Potomac Books.
- Armistead, E.L. (2010) *Information Operations Matters: Best Practices*. Washington, DC, Potomac Books.
- Arquilla, J. (1994) The strategic implications of information dominance. *Naval Postgraduate School Faculty and Researcher Publications*. Summer: 24–30.
- Brown, C. & Ainley, K. (2005) *Understanding International Relations*. Houndmills, Palgrave Macmillan.

- Buzan, B., Wæver, O. & de Wilde, J. (1998) *Security: A New Framework for Analysis*. Boulder, Lynne Rienner Publishers.
- Clark, B.R. (2010) Information operations as a deterrent to armed conflict. *Military Review*. May–June: 97–104.
- Clark, R.M. & Mitchell, W.L. (2018) *Deception: Counterdeception and Counterintelligence*. Washington, DC, CQ Press, an Imprint of SAGE Publications, Inc.
- House Permanent Select Committee on Intelligence (2018) *Report on Russian Active Measures*.
- International Telecommunication Union (2015) *Measuring the Information Society*. Geneva, International Telecommunication Union.
- Jones, A. & Kovacich, G.L. (2016) *Global Information Warfare*, 2nd edition. Boca Raton, CRC Press.
- Jowett, G.S. & O'Donnell, V. (2012) *Propaganda and Persuasion*, 5th edition. Thousand Oaks, Sage Publications, Inc.
- Larson E.V., Darilek R.E., Kaye, D.D., Morgan, F.E., Nichiporuk, B., Dunham-Scott, D., Thurston, C.Q. & Leuschner, K.J. (2009) *Understanding Commanders' Information Needs for Influence Operations*. Santa Monica, RAND Corporation.
- Lasswell, H.D. (1958) *Politics: Who Gets What, When, How: With Postscript*. New York, Meridian Books.
- Meserole, C. & Polyakova, A. (2018) Disinformation war. *Foreign Policy*. May 25.
- Muñoz, A. (2012) *U. S. Military Information Operations in Afghanistan. Effectiveness of Psychological Operations 2001–2010*. RAND Corporation.
- NATO Strategic Communications Centre of Excellence (2014) *Analysis of Russia's Information Campaign against Ukraine*.
- NATO Strategic Communications Centre of Excellence (2015a) *The Manipulative Techniques of Russia's Information Campaign*.
- NATO Strategic Communications Centre of Excellence (2015b) *Redefining Euro-Atlantic Values and Russia's Strategic Communication in the Euro-Atlantic Space*.
- NATO Strategic Communications Centre of Excellence (2016a) *Framing of the Ukraine-Russia conflict in online and social media*.
- NATO Strategic Communications Centre of Excellence (2016b) *Russian Information Campaign Against Ukrainian State and Defence Forces*.
- NATO Strategic Communications Centre of Excellence (2016c) *Social Media as a Tool of Hybrid Warfare*.
- Pape, R.A. (1996) *Bombing to Win: Air Power and Coercion in War*. Ithaca, Cornell University Press.
- Paul, C. (2008) *Information Operations – Doctrine and Practice: A Reference Handbook*. Westport, Praeger.
- Pomerantsev, P. (2015) The Kremlin's information war. *Journal of Democracy*. 26(4): 40–50.
- Pynnöniemi, K. & Rácz, A. (2016) *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine*. FIIA Reports, no. 45. Helsinki, Finnish Institute of International Affairs.
- Shaw, I.G.R. (2017) Robot wars: US Empire and geopolitics in the robotic age. *Security Dialogue*. 48(5): 451–470.
- Steele, R.D. (2006) *Information Operations: Putting the "I" back into DIME*. Darby, Diane publishing.
- Thomas, T.I. (2004) Russia's reflexive control theory and the military. *The Journal of Slavic Military Studies*. 17(2): 237–256.
- United Kingdom Ministry of Defence (2014) *Allied Joint Publication for Psychological Operations (AJP 3.10.1)* Edition B Version 1, dated SEP 2014 (with UK National Elements).
- United States Joint Staff (1996) *Joint Publication 3–13.1: Joint Doctrine for Command and Control Warfare (C2W)*.
- United States Joint Staff (2011) *Joint Publication 3–13.2: Military Information Support Operations*.
- United States Joint Staff (2013) *Joint Publication 3–12 (R): Cyberspace Operations*.
- United States Joint Staff (2014) *Joint Publication 3–13: Information Operations*. Dated 27 Nov 2012, incorporating change 1 dated 20 Nov 2014.
- Ventre, D. (2009) *Information Warfare*. London, ISTE Ltd.
- Waltz, E. (2007) Means and ways: Practical approaches to impact adversary decision-making processes. In Kott, A. (ed.), *Information Warfare and Organizational Decision-Making*. Norwood, Artech House, pp. 89–114.
- Washington Post* (2014) Obama dismisses Russia as 'regional power' acting out of weakness. (25 March)
- Zollmann, F. (2017) Bringing propaganda back into news media studies. *Critical Sociology*. OnlineFirst.
- Доктрина информационной безопасности Российской Федерации* (2000). *Doktrina informacionnoj bezopasnosti Rossijskoj Federacii* (2000).

- Доктрина информационной безопасности Российской Федерации* (2016). *Doktrina informacionnoj bezopasnosti Rossijskoj Federacii* (2016).
- Известия* (2015) 'От слов многополярном мире к делам'. *Izvestija* (2015) 'Ot slov o mnogopoljarnom mire k delam'. (29 September)
- Известия* (2016) 'Российская военная операция в Сирии: итоги и прогнозы'. *Izvestija* (2016) "Rossijskaja voennaja operacija v Sirii: itogi i prognozy". (15 March)
- Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года* (2013). *Osnovy gosudarstvennij politiki Rossijskoj Federacii v oblasti meždunarodnoj informacionnoj bezopasnosti na period do 2020 goda* (2013).

NATIONAL CYBER COMMANDS

Piret Pernik

Introduction

In the past decade, more and more states have started to acquire cyber military capabilities. Regardless of whether this process is labelled a cyber arms race or seen as part of military modernization, the increased capacity to inflict destructive effects on national critical infrastructure and armed forces' mission-essential functions is alarming from the point of preserving international peace and stability. Cyber capabilities are being used in every armed conflict, and it is believed that the side that uses them first may change the course of war for their benefit. Armed forces conduct cyberattacks outside a theatre and, on behalf of their governments, also against civilian targets. Moreover, according to Brose (2019) emerging technologies such as artificial intelligence, Internet of Things, quantum computing will change the way war is fought. Therefore, armed forces are seeking to modernize rapidly and adapt the traditional ways, means and ends of their strategies, policies and forces to the new operational domain, cyberspace.

In this context, in the past decade, over half of NATO member-states have publicly disclosed their intention to develop defensive and offensive cyber capabilities (Smeets, 2019). These public statements unveil countries' greater strategic ambitions in the cyber domain, which has spurred more investments into capability development. At the same time, at the present only few NATO countries have moved towards an actual operational capacity of military cyber force. Building an effective cyber force is a long-term, costly and complicated process (Smeets, 2018). Everyone – starting from servicemen at tactical and technical levels up to senior commanders – must understand the features of cyberspace, cyber capabilities and their implications for the mission. What opportunities, limitations, vulnerabilities and interdependencies do cyber capabilities bear? How do we integrate them into joint operations (US Army, 2018)? These are complex problems and as a result military cyber concepts are still underdeveloped and incomplete. Moreover, cyber commands need to find solutions to many practical problems, like how to attract talented people; how to access and develop toolsets for operations; what are legal limitations to operations; how to ensure interoperability with other force components (coordinating, de-conflicting and synchronizing), etc.

This chapter analyses national efforts in developing cyber command in five European small to mid-size countries: Estonia, Finland, Germany, the Netherlands and Norway. In

the discussion examples from greater Western military powers, France, the United Kingdom (UK), and the United States (US), are also presented. The chapter starts with a general overview of cyber commands, and explicates the following areas of the organizational development on cyber command: rationale for creation, organization, key missions, and political authorization of expeditionary operations.

General overview of cyber commands in the Euro-Atlantic region and beyond

National cyber command can be defined as a standalone military command, service or branch that directs and controls full spectrum (defensive, offensive and intelligence) cyber operations in and through the cyber domain. Offensive cyber operations are defined as applying force in and through cyberspace to disrupt, deny, degrade and destroy computer and information assets. Among five countries included into the analysis, Estonia, the Netherlands and Norway have cyber commands, Germany's cyber command can be considered military service, and Finland has a cyber defence division, but no cyber command.

Jamie Shea, then senior NATO official, estimated in 2010 that about hundred countries in the world were actively developing defensive and offensive cybers capabilities (Shea, 2010). However, according to the US intelligence community's late 2016 assessment, more than 30 countries were developing offensive cyber capabilities (Clapper et al., 2017). This number is likely to grow since cyber operations executed by Advanced Persistent Threat actors, which are often affiliated with militaries, and by the military organizations themselves, have occurred more frequently in the past years. For example, most recently, on 20 June 2019, the US cyber command (allegedly) disabled Iranian computer systems that controlled rocket and missile launches (Nakashima, 2019).

The scarcity of publicly available information limits analysing the precise scope of capabilities of cyber commands. At the present, the following 16 NATO members are said to have a cyber command: Belgium, Canada, Denmark, Estonia, France, Germany, Greece, Italy, the Netherlands, Norway, Poland, Portugal, Spain, Turkey, the UK, and the US. Belgium plans to establish military cyber component in 2019 (Smeets, 2019). In addition, according to media reports, the Czech Republic opened cyber command in Brno in January 2019 with initial operational capability planned as of 2020 and full operational capability as of 2025 (*Prague Daily Monitor*, 2018).

However, despite that plans in some of these countries (e.g. Italy and Poland) to establish a command have been disclosed, it remains unclear to what extent the entities are operational or are capable to conduct offensive cyber operations. A Belgian armed force's 2016 strategic document states that the armed forces 'will further develop its own cyber capability, consisting of a defensive, offensive and intelligence pillar'. The document notes that the military does not yet have offensive cyber capability but will develop it rapidly and provide the necessary investment budgets and additional personnel. This capability will be used in support of expeditionary operations (Vandeput, 2016). Other NATO members have created cyber commands but their mission is narrower than full spectrum cyber operations: for example, the Norwegian cyber command directs and controls only defensive cyber operations (Pernik, 2018).

On the other hand, 11 NATO members have not disclosed plans to create any military cyber organization such as cyber command, service, branch, or unit (Smeets, 2019). Except Croatia, Lithuania, and Luxembourg, these countries have not demonstrated a high level of cyber security. Some countries have not made public statements but may still make relevant

plans because their strategic documents recognize that the cyber domain is operational domain, for instance, Lithuania, Czech Republic and Slovenia (Smeets, 2019). The Netherlands created cyber command three years after the 2012 defence cyber strategy first disclosed that the Dutch government was developing military offensive cyber capabilities (Smeets, 2019). Likewise, France has considered cyberspace as an operational domain since 2008 but created cyber command nine years later in 2017 (Delerue et al., 2019).

It should be noted that few NATO member-states have specific strategic documents for cyber defence. While France published its cyber defence strategy in only 2019, the US Department of Defence issued its first, the National Military Strategy for Cyberspace Operations, in 2006 and the latest in 2018. (Here, one should note that the US directives for *information warfare* were already issued in 1992 and 1996.) The Netherlands has issued three iterations of defence cyber strategy (2012, 2015 and 2018), and Germany is developing a cyber defence concept (Pernik, 2018). Finland, technologically highly developed EU member-state has developed a classified a concept of cyber defence but (yet) without elevating its cyber operational arm, authorized to develop also offensive capabilities, to a command (Pernik, 2018.)

Beyond the Euro-Atlantic region, the People's Republic of China, the Islamic Republic of Iran, the People's Republic of Korea, and the Russian Federation are considered most capable and active actors in cyber economic and industrial espionage, as well as in conducting cyber operations. Their most advanced cyber capabilities reside within armed forces and military and civilian intelligence and security services. Academic scholarship and policy research are still lagging behind these real-life developments, and while research on military strategic thinking about information warfare in these countries exists, detailed accounts of the development of cyber forces is hard to find (Smeets, 2019). Moreover, Australia, Columbia, India, Israel, Singapore, South-Korea, United Arab Emirates and Vietnam are considered possessing substantial military cyberspace capabilities and some of these countries have announced intentions to create cyber commands and/or cyberattack capabilities (Pernik, 2018).

NATO members' cyber commands

In line with the 2014 NATO Wales Summit decision that significant cyberattacks can evoke an Article 5 collective response, and the following recognition in the 2016 Warsaw Summit that cyberspace is 'a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea' the Alliance started to develop cyber doctrine that is expected to be completed in 2019. In 2016 NATO started to integrate cyber operations into military planning and operations. In August 2018, NATO's Cyber Operations Centre (CyOC) at the Supreme Headquarters Allied Powers Europe (SHAPE) was created and it was announced that five members (Estonia, Denmark, the Netherlands, the UK, and the US) will contribute sovereign cyber effects to support NATO missions and operations (NATO, 2018; US Department of Defence, 2018). NATO's CyOC provides situational awareness and an operational level platform for integrating national capabilities with military operations.

It is expected that this progress will encourage more NATO members to create their own cyber commands, and there seems to be growing interest among them in sharing best practice.

Organizational development from initial to full operational capability may take many years, for example, eight years for the US cyber command. The end point of organizational development, or: maturity, is a moving target, because capabilities and training requirements need to be adapted to the constantly changing cyberspace. At the present, only the

US, France and Canada are approaching the second last stage (expansion) of five phases of organizational development of cyber commands, capacity to carry out offensive operations (Smeets, 2019). Among them, the US cyber command announced in May 2018 full operational capability of 133 cyber mission force teams (with an additional 21 teams planned to achieve that milestone in 2024). In the same month, the Command was elevated to a unified combatant command status. However, by the end of 2018 it still had failed to meet the set training readiness standards (United States Government Accountability Office, 2019).

Another framework which enables more profound assessment of military capabilities is a NATO framework known as DOTMLPFI, which measures capability development in nine areas: doctrine, organization, training, materiel, leadership and education, personnel, facilities, and infrastructure. The organizational development of cyber commands in five countries will be assessed later in this article according to this framework.

Rationales for creating cyber commands

Developing military cyber capabilities is generally considered necessary for maintaining freedom of action, information superiority, projecting military power, and denying these to an opponent. Cyber capabilities support military operations in the domains of air, sea, land, and space, and in certain cases they are thought to replace kinetic action with relatively comparable operational effects but without casualties. Creating a new organization dedicated to cyber operations can be advantageous even though it is not a predicament for launching offensive cyber operations.

First, most cyber commands struggle with funding. For instance, senior officers of the Estonian defence forces called in the late 2018 for greater investments into people, equipment and capabilities of the Estonian cyber command (Pernik, 2018). If a cyber commander is placed directly under country's most senior military officer, usually chief of defence, the command and control chain is shortened which enables quicker decision-making. Greater authority will yield additional possibilities to direct more investments into the development of cyber capabilities. A cyber command independent from other services can implement more innovative and flexible policies in the areas of personnel, procurement, and training (for instance, developing new career models, and speeding acquisition of equipment), compared to other services. Innovative policies are needed to build (recruit, retain, and train) cyber force; acquire equipment (tools and platforms), develop in-house technology, attract top talent, etc. When senior and operational commanders will better understand how cyber effects can support them, additional funding decisions will be more likely. On the other hand, such authority may, at least initially, create tensions among the established structures and chains of command. As it is essential to integrate cyber operations into joint planning and support, too short a command chain may rather isolate than integrate.

Second, some countries such as Estonia, Germany, and Norway created cyber commands because it was a way to centralize, consolidate, and streamline formerly fragmented ICT and cyber-related capabilities and organizations. This enabled eliminating overlapping roles and responsibilities, and a more efficient use of resources in the backdrop of declining defence spending in many countries (Pernik, 2018). As discussed in the introduction of this chapter, in the increasingly contested cyber domain armed forces are seeking for the effective ways to transform and adapt. A staff component within a cyber command, focusing on strategic and policy issues related to the cyber domain, is likely to facilitate these processes.

Smaller NATO members may also be incentivized to create a new organization in order to enhance cooperation with key allies. Close bi- and multilateral relations between cyber

commands can facilitate organizational development by improved sharing of information, best practices, and common approaches to reserve forces and training. Small countries such as Estonia and Denmark with modest intelligence and situational awareness, can build trust via NATO's CyOC platform with key allies.

Finally, the development of cyber capabilities is often presented in strategic documents as means of deterrence to either deny of other actor's cyberattacks or ability to punish after a such. The Netherlands 2018 cyber defence strategy perceives cyber command's capabilities as part of the overall cross-domain deterrence. It states that the operational capabilities 'contribute to the total arsenal of deterrence means available to the government. Deterrence makes the Netherlands a less attractive target for (cyber-)attacks and is above all a means for conflict prevention. In addition to the ability to attribute attacks, deterrence requires credible offensive capabilities' (Ministry of Defence, 2018). The Dutch international security strategy from 2018 also makes the same argument, viewing an attack-capability as a deterrent:

the government is also investing in cyber intelligence and in both defensive and offensive cyber capabilities to protect against, respond to and deter cyberattacks and espionage. With these capabilities, the Netherlands aims to detect and neutralise cyber threats at an early stage, repel them effectively and – in extreme cases – retaliate proportionately.
(Ministry of Foreign Affairs, 2018)

The argument can be made that by publicly admitting offensive cyber capabilities can disincentivize others from launching cyberattacks because counter-attacks could be costly. Healey (2018) has concluded that the reason why the Obama's administration did not respond to Russia's interference in the 2016 US elections could have been a fear of the US decision-makers of inviting more devastating attacks against voting machines. Indeed, in 2019 it was disclosed that the Russians had compromised vendors of voting machines and compromised voter registration systems in some states (Zetter, 2019).

Offensive capabilities also support deterrence because pre-emptive and counter attacks can be used to deny the perpetrator malicious activities. For instance, on one day of the 2018 US midterm elections, the US cyber operation temporarily disabled Russia's Internet Research Agency's access to internet. In the words of Buchanan (2019) it was 'an attempt to deny, temporarily removing an arrow from the Russian's quiver'.

To sum up, over half of NATO countries are creating cyber commands, and about the same number have revealed that their capabilities can be used for offensive operations. At the same time, NATO has found a way to incorporate voluntary offensive cyber capabilities into its defensive defence posture to support NATO missions and operations. These relatively recent developments are intended to strengthen the credibility of NATO members' deterrence in the cyber domain by affecting rational cost-benefit calculations of potential adversary nation-state, or affiliated, decision-makers.

Missions of cyber commands

With few exceptions, in the Euro-Atlantic region, cyber commands are assigned to three central missions: 1) defend military networks, systems, and assets against cyberattacks; 2) support military operations with cyberspace capabilities; and 3) support civilian authorities in defending the country against serious cyberattacks. In some countries the last mission includes defence of national critical infrastructure.

In the remaining sections, the approaches to building cyber forces in Estonia, Finland, Germany, the Netherlands, and Norway are compared with additional observations from France, the UK, and the US. All these countries, except Germany, state explicitly in strategic documents the development of offensive cyber capabilities. A 2016 German defence white paper recognizes that ‘cyberspace is increasingly becoming a theatre of conflict’ and ‘operations in the cyber and information domain are already playing an increasingly significant role in military conflicts.’ Yet, the offensive cyber capabilities are acknowledged only indirectly: ‘Germany must [...] work towards ensuring the unhindered use of ground, air and sea lines of communication as well as of space and the cyber and information domain’ (Federal Ministry of Defence, 2016).

Talking about the type of missions, cyber commands are generally responsible for ensuring the cyber security and the protection and operation of IT systems. Only in the Netherlands does this responsibility belong to the Computer Incident Response Capability (CIRC), which is not part of the command. Some cyber commands have authority to execute full spectrum (defensive, offensive, and intelligence) cyber operations (for instance, Germany, the Netherlands, the US). In some countries situational awareness and intelligence is additionally or in total provided by other departments of the armed forces (for instance, in Estonia by military intelligence).

Cyber commands oversee integrating cyber effects into the planning of military operations, usually in close cooperation with operation division and other relevant departments of the armed forces. In some countries (for instance, Finland) the cyber defence unit does not have primary responsibility in this area but supports the leading departments. In the Netherlands, cyber command seconds experts to the operations division. The Dutch cyber command prepares cyber operation mission teams consisting of a wide range of specialists (e.g. intelligence, technicians, and operational planning) that will be deployed at expeditionary operations under the command of an operational commander (Pernik, 2018). The US Army deploys at theatre level an even more comprehensive specialized detachment (integrating cyber, intelligence, information electronic warfare and space capabilities). At the operational and tactical levels (brigade, division, and corps) teams integrating cyber, signal and electronic warfare will be deployed under operational commanders (Pomerleau, 2019).

Interestingly, at present only a few countries have integrated information operations and electronic warfare with cyber operations under the authority of cyber command, most notably Germany. Estonia’s cyber command integrates information and cyber operations. In other countries analysed (Finland, the Netherlands, Norway, and the US), cyber commands do not include information operation and electronic warfare components or functions. However, in the UK and US operational level cyberspace capabilities are integrated with information environment and space-related capabilities. Moreover, the UK and US army doctrines integrate, synchronize, de-conflict, and coordinate cyber operations and electromagnetic activities (Ministry of Defence, 2018; US Army, 2018). In fact, several scholars and military officers emphasize that such an integration is inevitable for operating successfully (Libicki, 2017; Akerman, 2018).

Mission assurance aims to keep mission-essential functions and assets secure enough to reliably accomplish mission objectives. Similarly, mission assurance (as opposed to information assurance) is generally not a cyber function. In Estonia, one of the central missions of cyber command is to provide the work environment and organize command support for defence forces headquarters. (Previously, this function was the responsibility of Support and Signal Battalion that was integrated into the command in 2018.) In some countries (Estonia, Germany, and Norway) maintaining ICT services and infrastructure of the armed forces

is one of the key missions of the commands. According to the commander of the Estonian cyber command, the framework of IT life-cycle management is part of cyber command's functions (Hairk, 2018). However, the life cycle management approach does not address resiliency and redundancy aspects of mission assurance that focuses on continuous operation and executing mission successfully even when some systems fail.

As with any military command, cyber commands will also become responsible for the development of non-operational capability elements, in particular, personnel policies, and educating, training and exercises. The commands have started to design career paths and motivational packages, including student loans and scholarships, to better recruit and retain the workforce. In Estonia, the cyber command organizes the preparation of wartime and reserve forces, as well as conscript service in the area of cyber defence. Estonia and the Netherlands have cyber range in the cyber command, and the Netherlands has also a centre for excellence for research and competence development.

The staff components of cyber commands are engaged in the development of concepts and policies, often in cooperation with ministries of defence, but at the present doctrine, rules of engagement, legal framework for cyber operations, as well as response options and contingency plans are still underdeveloped.

Regarding national and international cooperation, cyber command serves as a designated point of contact for armed forces' cyber security matters, both for national and international partners and stakeholders. Developing these relations are generally considered a priority matter. However, as Finland's example demonstrates, cooperation with NATO CCD COE and NATO institutions can be established without creating a new, cyber-dedicated organization.

Organizational development of cyber commands

Smeets (2019) offers a life style framework in order to compare the degrees of maturity of a military cyber organization. The five stages of development are: seed, start up, growth, expansion, and maturity. In the seed phase it is recognized that a new organization is needed, start up refers to an official decision to launch it, in the growth stage operational capacity is being developed, in the expansion stage the capacity to carry out offensive operations exists and maturity is reached when the organization is able to conduct a full spectrum of operations against a wide range of targets and has an effective strategy in place. Accordingly, France and the US are among the most mature NATO members having passed to the expansion phase. The Netherlands reached the growth stage in 2018; Estonia and Germany are also in the growth stage (Smeets, 2019).

If we measure organizational development according to the NATO DOTMLPFI framework, the cyber commands of Estonia, Germany, and Norway have deficiencies in most of these nine capability areas, except organization.

Among the three, the Netherlands has progressed the most – as discussed earlier, it has a cyber defence strategy, an organization capable of full spectrum operations, a centre of excellence for research, a cyber range, and expeditionary cyber operation teams. Germany, on the other hand, exhibits the most comprehensive approach to capability development. The German cyber command has workforce of 13,000 and several facilities located across the country. It maintains a cyber reserve (which includes voluntary service) programme aimed at attracting members from technical and non-technical fields of professional activity (including board members and executives of technology companies). In cooperation with German universities, it provides academic degree programmes and has created a technology start-up hub in Berlin bringing together experts from government, research and industry

(German cyber command, 2019). It is expected that in the future, cyber commands are likely to be granted additional authority for acquisition of equipment (materiel).

Estonia has also a fairly lean organization, and a short command and control chain. It is developing and implementing training programmes for conscripts and other youth target groups (such as summer camps and technical competitions for school pupils, defence sector hackathons, scholarships for students, etc.). Finland's defence forces have likewise taken strides in developing a reserve system, education and training courses, exercises, as well as conscript service for cyber defence (Pernik, 2018). The Netherlands establishes standards for occupational profiles. Each position, e.g. unit commanders, operational planners, technicians, and operations centre operators) will have demanding training requirements.

Compared to these countries, Norway lags behind in development of doctrine, and education and training. While Norway's 2019 national cyber strategy prioritizes education and training of public and private sectors, and Norway joined NATO CCD COE in 2019, it has not embarked on specific programmes for cyber defence workforce development. The Norwegian cyber command, however, incorporates a cyber defence weapons school. Strategic guidelines for the development of Norwegian armed forces' cyber capabilities were issued in 2014 and have not been revised since. As a NATO member, Norway is obliged to fulfil NATO Cyber Defence pledge requiring members to allocate more resources to national resiliency measures. Norwegian armed forces also participate in international and NATO cyber exercises, such as Locked Shields, and NATO's Cyber Coalition and CMX, but the bulk of activities is focused on the security of IT systems (Norwegian Ministries, 2019). Hence, there is little development of actual operational capability.

The set-up of organization is predicated on how the cyber security-related organizations of armed forces will be combined and restructured. New organizations emerge from the existing organizational culture, and their formation is impacted by the broader societal and political context. Also, objectives of national security and defence policy, assessment of security threats, NATO-membership, and many other external factors, even personal preferences, may all affect the shape that the new organization will take. An example of rebranding is Norway where in 2012 the Information Infrastructure Organization was rebranded into cyber command which was elevated to the status of an independent institution (cyber command is one branch of the armed forces).

Some countries have included military CIRC into cyber command while others keep these functions separate. Germany and Norway have dedicated centres for cyber security and Computer and Information Security (CIS) services. The Norwegian 'Centre for ICT Services' (CIKT) is part of the cyber command that ensures IT services, infrastructures, networks, and systems of the armed forces (Pernik, 2018). The Dutch CIRC is an independent organization under the Defence Materiel Organization whose task is to ensure CIS and cyber security in the armed forces. The Dutch CIRC supports civilian stakeholders in the protection of critical national infrastructure. In Norway and Estonia cyber command and the Finnish cyber defence unit do not have mandate to support national critical infrastructure (Pernik, 2018).

To compare the organizational set-up of cyber commands in Estonia, Germany, the Netherlands, and Norway, in the first three countries cyber commands have a staff component and centres for operations and technology/software. Norway also has a cyber defence operations centre. In addition, Estonia and Germany have strategic communications departments separated from information operations functions. Intelligence and situational awareness components are present in Germany and the Netherlands.

Publicly available information about the funding of cyber commands is limited. Estonian government's budget for implementing the national cyber security strategy 2019–2022 is for the fiscal years of 2019 and 2020 €4.2 million (Government of Estonia, 2019), but how the amount will be allocated to different ministries and objectives is not publicly communicated. Likewise, the annual budget does not inform of expenditure on cyber defence. A similar example comes from Norway where the acquisition of ICT materiel and equipment is but allocations to cyber security are not communicated. (Ministry of Defence, 2019).

As national missions and priorities differ, direct comparisons of expenditures can perhaps only testify of different priorities. For example, while in 2017 Norway's cyber command's annual budget was a modest €197,000 (Pernik, 2018), Denmark allocates €9 million a year, Spain had allocated in 2014 €2.3 million, and the Netherlands allocates around €20 million a year on top of initial funding of €50 million. France disclosed in 2016 that it allocated €2.1 billion for cyber command (Smeets, 2019). Vastly different sizes of budgets indicate that capabilities of cyber commands are also very different.

The size of personnel may not necessarily reflect the actual operational capability, either but rather the overall tasks of the organization. For instance, in Germany by 2021 total manpower will be 14,500, but this number includes geoinformation data service, schools, and many other entities. However, cyber capabilities of France will increase remarkably – by 2025 it will have 4,000 'cyber combatants' (Ministry of Defence, 2018). In Estonia, the total manpower is expected to grow to 300 by 2023 and Finnish division employs about the similar number. Small budgets limit the ability of organization to grow (Smeets, 2019), however small countries can focus on developing specific, niche skillsets.

Political authorization of expeditionary cyber operations

Cyber threats cross physical borders and jurisdictions and a concept of cyber perimeter defence has become outdated. Accordingly, the 2018 US DoD cyber defence strategy and the US Cyber Command's vision prescribe 'defending forward', that is outside their own networks, as a defining element of national security. The primary concern for smaller countries with more modest operational focus will be defending their own systems and infrastructures against cyberattacks in their own territory (Pernik, 2018). At the same time, in 2018 Estonia announced its readiness to contribute national cyber capabilities to support NATO missions and operations, which curiously may indicate that such capabilities already exist (ERR News, 2018). From a small country perspective, contributing to NATO's CyOC is a way to maintain close relations with the main NATO allies of US and UK, and potentially increase its competence and improve situational awareness. Smaller countries rely on the superior intelligence capacity their bigger allies and partners possess.

In order to deploy cyber capabilities at expeditionary operations, including NATO missions and operations, as a rule a decision must be taken by the highest political levels – government (the Netherlands and Norway), president (Finland) or parliament (Estonia and Germany). The mandate would be limited to a contingent situation, certain geographic location, and timeframe. It is anticipated that as cyber commands will continue to expand and mature, national regulators are going to amend legislation to simplify the deployment process. Many countries have enacted new legislation granting greater authorities to intelligence services and law enforcement in network surveillance, interception, and in certain cases right to disconnect end-users.

The Netherlands has already taken this step in regards to the armed forces. In the case of deployment of cyber capabilities at international missions, the Dutch government has the

capacity to decide, and it would, as ascertained in the Dutch constitution, article 100, inform the public. This information includes an explanation about the role of cyber capabilities in the mission (Ministry of Defence, 2018). The Netherlands considers that greater public transparency about the use of cyber capabilities will help to raise awareness about the fact that cyberspace is an operational domain (*ibid.*).

In general, NATO members contributing sovereign effects to NATO missions and operations, national capabilities would be commanded by national commanders, but integrated with NATO operations through NATO's CyOC. In other words, these cyber operations will not be executed under the command of Supreme Allied Commander Europe (SACEUR) and subordinate NATO commanders as is the case with other NATO operations. The exception is the US, because the commander of the US European Command fulfils also the position of SACEUR, and he could be granted a commanding authority of the US Cyber Command (Freedberg, 2018).

Conclusion and observations

This chapter has analysed the development of cyber military capabilities in the West from the perspective of the establishment, development, and tasks of national military cyber commands. The decision to create a new organization, and its particular set-up is conditioned by internal factors – e.g. organizational and administrative culture and established structures and practices – and from the wider social and political context where a wide array of factors ranging from available funding to understanding of cyberspace to security and defence policy ambitions and objectives play a role. This analysis highlighted the degree of variance among cyber commands. They are differently mandated, tasked, organized and, obviously, manned and funded. The growth of organizations has taken longer than anticipated. It may well be that monetary concerns are secondary to doctrinal challenges and shortages of professional manpower. Countries with cyber commands are likely to progress faster in developing concepts and doctrines; indeed, one could even ask what is the purpose of establishing a command without a doctrine?

Based on the comparison of the cyber military commands of Estonia, Finland (in this case division), Germany, the Netherlands, and Norway, it can be extrapolated that 'an ideal model of cyber command' appears to be a fairly lean organization, subordinated to the chief of defence in peacetime and under operational or tactical command of a joint/operational commander during operations. At minimum, a cyber command should be composed of staff sections (capabilities) for strategic and policy analyses and planning (including legal and technological development), intelligence, situational awareness, operational planning, conduct of cyber operations. Cyber command should be supported by a military centre of excellence for research and competence, as well as a cyber range. Finally, the command should have a degree of authority for acquisition and personnel policies (including reserve forces and conscription if applicable), as well as education, training, and exercises.

The advocates of cyber military commands praise the deterring effect cyber commands can create. They can consolidate previously separated entities and facilities under the same banner. As the primary stakeholders, cyber commands have core responsibility to develop their field – military cyber defence. Here, the critics of proliferation and 'arms races' warn of the destabilizing or escalatory effects adherence to military security may inflict. Unless the mere existence of cyber military capabilities, cyber commands included, lowers the threshold to project national military power, cyber commands remain pawns rather than kings on a chessboard.

References

- [illegible]

- Ministry of Defence [Norway] (2019) *Future Acquisitions for the Norwegian Defence Sector 2019–2026* (28 February). Available from: www.regjeringen.no/en/dokumenter/future-acquisitions-for-the-norwegian-defence-sector-2019-2026/id2630912/ [accessed 1 July 2019].
- Ministry of Defence. [Netherlands] (2018) *Defensie Cyber Strategie 2018. Investeren in digitale slagkracht voor Nederland*. November 2018 (unofficial translation by Matthijs Koot). Available from: www.defensie.nl/downloads/publicaties/2018/11/12/defensie-cyber-strategie-2018 [accessed 30 June 2019].
- Ministry of Defence [UK] (2018) *Joint Doctrine Note 1/18. Cyber and Electromagnetic Activities* (February 2018). Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf [accessed 30 June 2019].
- Nakashima, E. (2019) Trump approved cyber-strikes against Iran's missile systems. *Washington Post* (22 June). Available from: www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html?noredirect=on&utm_term=.88ee6a6e3d11 [accessed 30 June 2019].
- NATO (2017) *AJP-6. Allied Joint Doctrine for Communication and Information Systems*. Edition A. Version 1 (1 February). Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/602827/doctrine_nato_cis_ajp_6.pdf [accessed 30 June 2019].
- NATO (2019) *The NATO Command Structure Factsheet*. NATO, February 2018. Available from: www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/1802-Factsheet-NATO-Command-Structure_en.pdf [accessed 30 June 2019].
- Norwegian Ministries (2019) *List of Measures – National Cyber Security Strategy for Norway*. Available from: www.regjeringen.no/en/dokumenter/national-cyber-security-strategy-for-norway/id2627177/ [accessed 1 July 2019].
- Pernik, P. (2018) *Preparing for Cyber Conflict – Case Studies of Cyber Command*. International Centre for Defence and Security (December). Available from: https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf [accessed 1st July 2019].
- Pomerleau, M. (2019) How the Army is taking cyber units to the battlefield. *Fifth Domain* (13 March). Available from: www.fifthdomain.com/dod/army/2019/03/13/how-the-army-is-taking-cyber-units-to-the-battlefield/ [accessed 1st July 2019].
- Prague Daily Monitor* (2019) Czech military cyber forces might have headquarters in Brno (17 July). Available from: www.praguemonitor.com/2018/07/17/czech-military-cyber-forces-might-have-headquarters-brno [accessed 30 June 2019].
- Pritchett, M.D. (2012) *Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating in a Contested Cyber Environment*. Available from: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a563712.pdf> [accessed 30 June 2019].
- Shea, J. (2010) *Lecture 6- Cyberattacks: Hype or an Increasing Headache for Open Societies?* (2 February). Available from: www.nato.int/cps/en/natolive/opinions_84768.htm [accessed 30 June 2019].
- Smeets, M. (2018) Integrating offensive cyber capabilities: meaning, dilemmas, and assessment. *Defence Studies*. 18(4): 395–410. Available from: <https://doi.org/10.1080/14702436.2018.1508349> [accessed 30 June 2019].
- Smeets, M. (2019) NATO members' organizational path towards conducting offensive cyber operations: A framework for analysis. In Minarik, T., Alatalu, S., et. al. (eds), *2019 11th International Conference on Cyber Conflict: Silent Battle*. Tallinn, NATO CCD COE.
- US Department of Defense (2012) *Mission Assurance Strategy*. Washington, DC. Available from: https://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf [accessed 30 June 2019].
- US Army (2018) *Cyberspace and Electronic Warfare Operations. FM 3–12*. Washington, DC: U.S. GPO (11 April).
- US Army (2018) *The U.S. Army Concept for Cyberspace and Electronic Warfare Operations (2025–2040). TRADOC Pamphlet 525–8-6*. Available from: <http://adminpubs.tradoc.army.mil/pamphlets.html> [accessed 30 June 2019].
- US Cyber Command (2019) *US Cyber Command History*. Available from: www.cybercom.mil/About/History/ [accessed 30 June 2019].
- US Department of Defence (2018) *News Conference by Secretary Mattis at NATO Headquarters* (October 4). Available from: <https://dod.defense.gov/News/Transcripts/Transcript-View/Article/1654419/news-conference-by-secretary-mattis-at-nato-headquarters-brussels-belgium/> [accessed 30 June 2019].

- United States Government Accountability Office (2019) *DOD Training. U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force. Report to the Committee on Armed Services*. House of Representatives (March). Available from: www.gao.gov/assets/700/697268.pdf [accessed 2nd July 2019].
- Vandeput, S. (2016) *The Strategic Vision for Defence*. Minister of Defence (29 June). Available from: www.mil.be/sites/mil.be/files/pdf/strategic-vision-belgian-defense-en.pdf [accessed 30 June 2019].
- Zetter, K. (2019) Software vendor may have opened a gap for hackers in 2016 swing state. *Politico* (6 May). Available from: www.politico.com/story/2019/06/05/vr-systems-russian-hackers-2016-1505582 [accessed 30 June 2019].

PART III

National and regional perspectives on cybersecurity

Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

CYBER CAPACITY-BUILDING AND INTERNATIONAL SECURITY

Souhila Amazouz

Introduction

The rapid advancement of Information and Communication Technologies (ICTs) and the enormous transforming power of cyber space has reshaped the international security environment (UNGA, 2013, #6). The security of cyberspace is now at the top of the agenda of all-important international meetings in both bilateral and multilateral discussions. While initiatives are underway both at regional and global levels exploring ways to ensure security and stability of this new strategic space, a special interest is given to state responsibility and accountability in the use of ICTs. For instance, conversations related to the development of international cybersecurity norms and code of conduct in cyberspace started in the United Nations in 1998 when Russia introduced the first draft resolution on the use of ICTs by states in the context of international security. This initiative resulted some years later in the establishment of UN Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) and also paved the way for formal discussions on cyber related issues at the UN General Assembly and also at UN specialized organizations and agencies.

Since 2004, the UNGGE reports and respective resolutions aim at promoting secure, stable and peaceful digital environment for all people and states across the world. The awareness on the link between cyber threats and international security was also highlighted in several UN reports, for example in 2010 it was clearly indicated that ‘there is increased reporting that states are developing ICTs as instruments of warfare and intelligence, and for political purposes’ (UNGA, 2010, #7).

However, after years of multilateral discussions under the auspices of the UN, the search for a global approach to the security of cyberspace remains a challenge for the international community. And this despite the general recognition of the importance of international cooperation to mitigate cyber risks which was highlighted by relevant organizations and states in their cybersecurity policies. On the other hand, in response to cyber threats, organizations and states are placing a growing importance on cyber capacity development as a key element for enhancing transparency and predictability of behaviour in cyberspace to avoid misperceptions and counter cyber incidents and criminal cyber operations (Van der Meer, 2016).

This chapter situates the main global and regional cyber capacity-building initiatives in the context of international peace and security. It calls for the peace, security, and stability of cyberspace to be achieved not only by international norms, rules and principles but by promoting capacity-building and dissemination of best practices among states across the world.

Calling for capacity

Nowadays, major cybersecurity initiatives and forums across the world emphasize the criticality of building cyber capacity to lay the foundation for resilient and secure digital ecosystem. For example, the Global Commission on the Stability of Cyberspace (GSCC), the Global Forum on Cyber Expertise (GFCE), the Geneva dialogue, The Internet Governance Forum (IGF) and quite recently the Paris Call for Trust and Security in Cyber Space all aim for developing comprehensive cyber capacity programmes to benefit people and states all over the world.

Cyber capacity-building is related to all activities that aim to safeguard and promote safe and open use of cyberspace including legal and institutional reforms, policy and strategy development, improving technical and organizational capacity and human skills and competences as well as the organizational adaptation of existing institutions and agencies to the reality of digital environment (Pawlak, 2014, p. 6)

Since the beginning of the formal multilateral discussions at the UN level, all Groups of Governmental Experts have emphasized the need to promote cyber capacity-building as a topic of general consensus among the members. Indeed, despite divergent views on international cybersecurity policy between the western countries from one side and Russia, China and their allies on the other, due mainly to the lack of common understanding on state accountability in the use of ICTs as well as the absence of global agreement on the applicability of certain international laws in cyberspace (Korzak, 2017, cf. Tikk & Kerttunen, 2018), developing cyber capacities and competencies remain the least controversial topic in international cybersecurity policy (Kurbalija, 2018, p. 8).

For instance, the GGE report of 2010 considers capacity-building of vital importance to achieve success in ensuring global ICT networks security. In addition, the report stressed on the need to assist developing countries in their efforts to enhance the security of their critical national information infrastructure and called for international cooperation to identify adequate measures and programmes to support capacity-building in less developed countries (UNGA, 2010, #17)

The GGE report of 2013 focused more on promoting regional and international capacity-building efforts to secure cyberspace, such as strengthening national cybersecurity frameworks and strategies, building law enforcement capabilities and assisting developing countries in managing ICT security incidents through facilitating transfer of knowledge and best practices. (UNGA, 2013, #32)

On the other hand, the World Summit on Information Society (WSIS+10) outcome document of 2015, Resolution 70/125, called upon states to intensify efforts to build robust domestic security in information and communications technologies in line with their international obligations and domestic law. In this regard, a special focus was given to capacity-building, education, knowledge-sharing, and raising the awareness of the general public to overcome challenges related to building trust and confidence in the use of ICTs and networks to sustain the national resilience and security (UNGA, 2015b)

However, the security of global cyberspace requires all nations to achieve a same level of understanding of rules and responsible use of cyber technologies. According to Microsoft,

‘critical to the success and impact of any cybersecurity norms will be their implementation’, yet this may be a challenge for developing countries to effectively implement globally accepted cyber norms as they lack technical know-how and financial resources to secure their cyber networks (Microsoft, 2019; cf. Tikk, 2017).

In addition, the Council of the European Union’s conclusions on external cyber capacity-building (EU, 2018b, p. 5) stressed the need to develop minimum capacities to effectively implement the regional cybersecurity confidence building measures (CBMs) as well as for the applicability of norms and principles of responsible state behaviour in cyberspace as set out in the UNGGE reports of 2013 and 2015. The development of cyber confidence-building measures has commenced within the regional organizations, the OAS (2009), the OSCE (2013, 2016), and the ASEAN Regional Forum (2015).

While many cyber capacity-building initiatives are underway to provide either policy guidance, technical assistance or financial support to strengthen institutional and organizational capacities of states in the field of cybersecurity. Achieving the secure and responsible use of cyber technologies by all actors including governments, private companies, and individuals is a shared responsibility and common objective to fully harness the potential and opportunities of the digital revolution.

The cybersecurity gap between developed and developing countries

There are substantive differences in cybersecurity frameworks and practices across the world. This increases vulnerability of ICT networks and create challenges for achieving common perspectives for the security and resilience of cyber domain.

The International Telecommunication Union (ITU) observes and compares the overall commitment of its 193 Member States to cybersecurity through the ITU Global Cybersecurity Index (GCI). The GCI is part of Resolution 130, which was updated in 2018, on strengthening the role of the ITU in building confidence and security in the use of ICT. The latter is considered as a capacity-building tool that can be used by states to identify areas of weakness requiring improvements. (ITU, 2018, p. 11)

According to the ITU Global Cybersecurity Index 2017, the top five countries of high commitment to cybersecurity in the world are Singapore, USA, Malaysia, Oman, and Estonia. However, the report revealed also significant disparities in cyber engagement of states across the world as less than 50% of states have adopted their national cybersecurity strategy (ITU, 2017). This is essentially due to the gap among countries and regions in terms of technological advancements, cybersecurity capacities, knowledge and awareness of the risks associated with the malicious use of cyber technologies. By mid-2019, it is reported that 107 countries have issued a national cyber or information security strategy (Kerttunen & Tikk, 2019).

So far, various methods have been used to review and assess the cybersecurity readiness of states across regions. For instance, the Global Cyber Security Capacity Centre (GCSCC), University of Oxford, as an international centre for research into efficient and effective cybersecurity capacity-building, has created the National Cybersecurity Capacity Maturity Model (CMM) to review cybersecurity capacity maturity of countries. This model has been deployed and tested in cooperation with other partners (including the Organization of American States, the World Bank, the Commonwealth Telecommunications Organization and the International Telecommunication Union) in more than 40 countries around the world and (GFCE, 2016b, p. 12)

From Africa, Senegal partnered with Netherlands and benefited from expertise of the Global Cyber Security Capacity Centre (GCSCC) of Oxford University, to assess and

evaluated its national cyber capacities using the Cybersecurity Capacity Maturity Model (CMM). The initiative was under the GFCE capacity-building initiatives and resulted in the adoption of the national cyber security strategy of Senegal one year later. (GFCE, 2016c, p. 10)

On the other hand, the UN Institute for Disarmament Research (UNIDIR, 2013) took a step towards mapping out the technical and political levels of the cyber capabilities of individual countries by organizing all countries according to the level and structure of their cyber capacity and security.

While many European and North American countries are well advanced in developing national cybersecurity as well as cyber defensive, offensive and intelligence capabilities, African and Asian nations are among the less digitally developed and therefore the most vulnerable to cyber threats.

In Africa, the majority of countries are at an early stage of developing their cybersecurity capacities as they focus more on deploying their digital infrastructures, digitalizing strategic sectors, and developing their digital economies to enable their people to participate in the digital world. As highlighted by Pawlak (2014), most African countries have already adopted their digital transformation agenda as a great opportunity for change and progress without taking into account the associated cyber threats.

According to Symantec report (2016), the cybersecurity landscape in Africa is marked by some cyber leading countries – such as Egypt, Kenya, Mauritius, Morocco, Rwanda, South Africa, and Tunisia – while the majority are at early stage of developing policy instruments and legislative frameworks to secure their cyber space. Moreover, the lack of cybersecurity skills to monitor and respond to cyber-attacks either originated from inside or coming outside their jurisdictions is real challenge for the majority of African countries as only 18 have set up a national computer emergency response entity.

International and regional cybersecurity capacity-building programmes

Cyber capacity-building has become of strategic importance in cyber affairs. It is highlighted in many initiatives, decisions and programmes aiming to address the disparities on cyber security preparedness among states, regions and also non-state actors. Therefore, developing security measures together with cybersecurity analytical and decision-making capabilities of states may play an important role in avoiding escalation of cyber conflicts and proliferation of malicious activities in cyberspace. Moreover, Barmpalou (2016) stresses that responding to the cyber needs of developing countries is of high importance to ensure the security and stability of global cyberspace (p. 25).

However, as highlighted by Pijenburg Muller (2015), the complexity and multi-disciplinary nature of cybersecurity makes it challenging for both states and partners to identify and implement adequate cyber capacity measures that can be tailored to each country and region (p. 7). She further noted that approaches and focus areas in providing cyber capacity support and assistance vary between states and regions. While some organizations and partners prioritize the assessment of all levels and cyber security areas within a country, others map out the differences in each country or focus only on specific aspect of cyber capacity such as strengthening legal frameworks or establishing national Computer Emergency Response Teams (CERTs) such as ITU programme on CERTs (Pijenburg Muller, 2015). While a number of initiatives are underway across the world to strengthen trust and security in cyber domain, Panagiota (2015) reminds the need of consistent coordination among different institutions and organizations to effectively use resources and avoid fragmentation of efforts (p. 25).

Many advanced states and organizations envision building cyber capacities of partner countries as an investment and a cornerstone of their international engagement to ensure global prosperity in the digital environment. For instance, the USA, Australia, the European Union, and China have included cyber capacity-building in their international cyber strategies.

Considering cyber capacity-building as a dimension and building block of cyber diplomacy (EC, 2018), some states have already engaged bilaterally and through multilateral organizations to enhance their cyber capacities, while the majority still rely on programmes being offered by international, inter-governmental and regional organizations such as the African Union Commission and its Regional Economic Communities; the Association of Southeast Asian Nations (ASEAN); the Council of Europe; the European Union; the League of Arab States; the Organization of American States; the Commonwealth Organization, the Organization for Economic Co-operation and Development (OECD) as well as the United Nations and its agencies.

The European Union, and Council of Europe

The European Union considers investing in developing cyber capacities of partner countries as a top priority. Already the 2013 ‘Cybersecurity Strategy of the European Union’ clearly outlines the importance of external assistance for developing cyber capacity of third countries to promote security, respect of rule of law as well as the protection of human rights in the global cyberspace. (EC, 2013, pp. 14–16). The EU supports the strengthening of political, technical, institutional, legal and regulatory cybersecurity frameworks in third countries as the best way to prevent the creation of safe havens for cybercriminals in developing countries. Moreover, promoting cyber capacity-building serves as a strategic building block of the evolving cyber diplomacy. (EC, 2013 and 2018, p. 37; EU, 2018a and 2018b)

In an effort to strengthen international cooperation in fighting transnational criminal activities committed over ICT and Internet networks, the Council of Europe (CoE) with support of the European Union is continually assisting countries to strengthen their criminal justice and law enforcement agencies. This support is to enable governments to efficiently respond to cyber incidents and also enhance their abilities to effectively participate in international cooperation and exchange of information on cyber threats and vulnerabilities. In this regard, the Cybercrime Programme Office of the Council of Europe (C-PROC) is responsible for the implementation of several capacity-building programmes such as: The Global Action on Cybercrime Extended programme (Glacy+) which is structured around specific objectives notably the adoption and implementation of cybercrime policies, strategies and legislation as well as building law enforcement criminal justice capacities (CoE, 2019). As the initiative aims at promoting Budapest Convention as the international instrument enabling cooperation among states to fight against cybercrime, it contains wider political objectives, too.

The Organization of American States

The Organization of American States (OAS) was the first regional body to adopt, in 2004, a Cyber Security strategy called ‘The Comprehensive Inter-American Cyber Security Strategy’ which provides a mandate to OAS General Secretariat to assist Member States in strengthening their cyber security capabilities (OAS, 2004).

Other cyber capacity initiatives in the region include the creation of the hemispheric watch and warning network, CISRTAmericas.org, aiming at strengthening incident

response capabilities through providing guidance and technical support to cyber security technicians from and around the region (Subero, 2018), issuing a guidebook on the creation and deployment of a national CSIRT, launching a Toolkit on Cybersecurity Awareness campaign as well as publishing cybersecurity readiness assessment reports in 2014 and 2016 (GFCE, 2019b).

Furthermore, to assist countries in the region to build their cyber capacities, OAS mandated the Inter-American Committee against Terrorism (CICTE) secretariat to organize technical trainings, policy roundtables, crisis management exercises, and also to promote cybersecurity cooperation in the region by facilitating exchange of best practices and relevant information on the security of networks and information systems (OAS, 2019).

The African Union, and Regional Economic Communities

During the last decade, Africa has seen a tremendous growth in developing ICT infrastructures and increasing Internet access. This progress exposes African countries to new opportunities, but also new challenges, as not all African countries are ready to face the challenges of the digital era.

In 2014, the AU 23rd Assembly of Heads of State and Government, adopted The African Union Convention on Cyber Security and Personal Data Protection which shows the commitment of African leaders to the promotion of cybersecurity in Africa. In 2017, Ministers of ICT and Communication of the African Union tasked the AU Commission to organize a yearly conference on cybersecurity, to establish a continental cybersecurity awareness month and to provide necessary support to AU Member States to develop national cybersecurity frameworks including cyber strategies, adequate cyber legislations and incident response mechanisms (AUC, 2017). In January 2018, the African Union leaders reiterated their engagement to fight against the criminal use of ICTs and pledged to work together to enhance cyber cooperation among AU Member States and added cyber security to the top priorities of the Union (AUC, 2018a).

Even though, there is not yet a comprehensive and coordinated cybersecurity capacity-building programme that can be implemented across the continent, it is worth noting that various cyber capacity-building activities have been conducted so far by the African Union Commission in collaboration with Regional Economic Communities, partners and international cyber security specialized institutions. For instance, the AU Commission in collaboration with US Department of State organized several regional workshops (2011–2016) with the aim of promoting cybersecurity due diligence in Africa, build cyber capacity and sensitize on the negative implications of cyber incidents that may undermine the use of digital technologies for national development (GFCE, 2016). Furthermore, in an effort to assist AU Member States in developing their national cybersecurity frameworks, the AU Commission in collaboration with the US Department of State, organized a capacity-building workshop in 2018 dedicated to cyber strategies, cyber legislations, and setting up of a national CERT/CIRT (AUC, 2018b).

The AU Commission hosted the first African Forum on Cybercrime in 2018, co-organized with the Council of Europe, gathering senior African officials, policy makers as well as experts from criminal justice authorities, law enforcement agencies, and judiciary and prosecution services. As part of the forum, workshops on cybercrime and electronic evidence as well as trainings on cybercrime strategies were provided to participants (CoE, 2018).

With regard to cyber policy dialogues and international discussions, the AUC has organized several capacity-building workshops on cyber diplomacy. These workshops aim

to equip African diplomats with the necessary knowledge that will enable them to follow and participate in international cybersecurity policy discussions and better promote African nations' interests in cyberspace (ICT4Peace, 2016).

African Regional Economic Communities (RECs) have worked within Africa sub-regions to strengthen the cybersecurity capacities of African governments and institutions. For example, the Economic Community of West African States (ECOWAS) has partnered with Council of Europe, Global Prosecutors E-crime Network (GPEN) of the International Association of Prosecutors (IAP) and the US Department of State to improve cybercrime legislation, national cybersecurity strategies and build capacities of prosecutors and investigators on fighting cybercrime (ECOWAS, 2017); and the Secretariat of the Southern African Development Community (SADC) convened a capacity-building workshop on Cyber Security and SADC Regional Cyber Drill in 2018 to enhance the cyber-threat preparedness of SADC Member States (SADC, 2018).

The Association of South East Asia Nations, and ASEAN Regional Forum

The diplomatic engagement for cyber capacity-building within the Association of South East Asia Nations (ASEAN) and Regional Forum (ARF) has been addressed in several regional processes. For instance, the Council for Security Cooperation in Asia Pacific (CSCAP) committed to 'Ensuring a Safer Cyber Security Environment' by signing a memorandum (No. 20) where they agreed to implement capacity-building and technical-assistance measures in the region with special focus on strengthening capability of crisis management and incidents response of all states through the development of the Asia Pacific CERT (APCERT) to facilitate regional cooperation and coordination amongst CERTs and CSIRTs (CSCAP, 2012). The 'ASEAN Network Security Action Council' (ANSAC) promotes the establishment of common network security framework with particular emphasize on capacity development for enhancing maturity level of CERTs (Abdul Wahab, 2016, p. 19). On the other hand, the 'ASEAN Cyber Capacity Program' (ACCP), launched in 2017, enables participation of different stakeholders to effectively identify and respond to specific needs of individual countries. ACCP aims to strengthen cybersecurity landscape of ASEAN members and enhance the ability of the region to respond to increasingly sophisticated cyber threats. (ASEAN, 2016, Prashanth, 2016)

The Global Forum on Cyber Expertise

The annual Global Conference on Cyberspace Conference (GCCS), also known as the 'London process', initiated, in the 2015 Hague Declaration, the creation of the 'Global Forum on Cyber Expertise' (GFCE), a global multi-stakeholder and coordinating platform that aims at facilitating exchanges of best practices and expertise on cyber capacity-building among all cyber actors. The platform is open to participation of state and non-state actors and encourages dialogues on implementation of global cyber capacity-building programmes from donor's and recipient's perspective to optimize the use of resources and avoid duplication of efforts (GFCE, 2019a).

To promote inclusive international cooperation on cyber issues, GFCE Members endorsed a 'GFCE Global Agenda for Cyber Capacity Building' (GACCB) in 2017. Among the key themes taken to support international security include policy commitment to cybersecurity, the establishment of incident management and response systems that enable nations to

respond and recover from cyber-attacks, the protection of critical infrastructures, adoption of effective cybercrime legislations, support the development of international cybersecurity standards as well as raising awareness on cyber risks and vulnerabilities that may hinder the individual and collective responsible behaviour in cyberspace (GFCE, 2017). Furthermore, the GACCB initiative is complemented with GFCE portals that provide an overview of regional and international cyber capacity-building initiatives and programmes as well as information related to cybersecurity readiness of countries across the world (GFCE, 2019c).

International Telecommunication Union

The 2005 World Summit on Information Society (WSIS) played a critical role in bringing Internet governance and cybersecurity to international discussions both at the technical and political levels. Moreover, this summit granted the International Telecommunication Union (ITU) the privilege to follow up on cybersecurity matters with its states members notably what is related to building confidence and security in the use of ICTs (ITU, 2005).

As a result, the ITU created the High Level Expert Group on Cybersecurity and launched the Global Cybersecurity Agenda (GCA) in 2007 as initiatives to enable and facilitate international cooperation among cyber actors to effectively fight against illicit cyber activities that can have negative impact on international security and stability of states (Toure, 2011, p. 104).

The ITU remains active in dealing with cybersecurity at international level and has developed several cybersecurity solutions and standards as well as a number of activities and programmes for building cyber capacities of developing and less developed countries. It is worth noting that the ITU offers valuable support to many countries across the world to develop their technical and operational cybersecurity frameworks such the CIRT programme which has been implemented since 2011 (ITU, 2019).

Conclusion: impact of cybersecurity capacity-building on international security

The security and stability of cyberspace is a conditional factor of any digital development and of the economic prosperity of nations. Cyber incidents, malicious cyber operations, and the lack of public awareness of cyber related risks may result in spreading mistrust and the non-adoption of digital technologies and services as enablers of socioeconomic development. Moreover, as stated in the 2010 GGE report, disparities in technological developments and ICT security capacities, as well as differences in national cybersecurity laws and practices, increase the vulnerability of the global network (UNGA, 2010, #11). This political, legislative, operational, and technical divide impacts negatively on countries' and regions' readiness to fight against the use of digital technologies for criminal and terrorist purposes.

According to Ghernaouti-Hélie (2010) cyberspace as a common space 'requires coordination, cooperation and legal measures among all nations to function in a smooth way like other domain (air, land, sea and outer space)'. However, to adopt a cybersecurity treaty that governs global cyberspace, countries need to be at the same level of cybersecurity maturity to actively participate in negotiations process and also to effectively implement the measures outlined in the treaty to ensure security of cyberspace and maintain international peace and stability.

As indicated in the 2015 GGE report, states' accountability in cyberspace requires them to meet their international obligations, perhaps most notably by not allowing the use of their territories by non-state actors to conduct malicious cyber operations to attack or damage

critical infrastructure in other states (GGE, 2015a, #13). Furthermore, as highlighted in the 2013 GGE report, ‘State sovereignty and 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’ (UNGA, 2013, #20). To enable nations to comply with their international obligations in securing their national cyberspace, respect both the human rights and rights of other countries and avoid escalation of cyber activities and incidents that may endanger international peace and security, it is important for all nations to meet an appropriate level of cybersecurity capacity to secure, monitor and manage their ICT networks and infrastructures and the related smart and interconnected services.

To enable the use of ICTs for good purposes – such as improving people’s lives and enabling new developments – there is a need to establish inclusive and consultative processes to reach global consensus on principles and rules to govern cyberspace and preserve it from cyber conflicts and tensions stemming from the illicit use of digital technologies.

The complexity of cyber security ecosystems and the lack of cooperation among different cyber communities (policy, technical, judiciary, civil society, private sector, and military) within and between countries contributes significantly to the creation of challenges related to security and trust in the use of digital infrastructures and services.

The relation between cybersecurity and international peace and security is recognized and highlighted in many reports. For instance, UN Secretary-General Guterres predicts that future wars will begin with ‘massive cyber-attacks’; he further expressed concerns about the continuous rising of cyber threat levels and absence of adequate international response such as international legal framework to address the growing risks of cyberwarfare and protect countries from severe cyber-attacks (Chong, 2018)

Yet, while all the UN Government Expert Groups since 2004 have agreed on cyber capacity-building as topic of general consensus, it is worth noting that no relevant programmes or initiatives were implemented towards assisting developing and less developed states and regions in building their cyber security capacities. Consequently, any failure in undertaking global and concerted efforts to build the cyber capacities of all nations, regions, and stakeholders across the world may result in creating cyber havens for international criminals and terrorists.

Since the cyber domain is a space without boundaries and cyber-attacks can affect both developed and developing countries, the damage may be even bigger for the less developed nations as they don’t have the necessary security measures and means to monitor and defend their digital infrastructures and systems. In this regard, laying the foundations for safe and secure global cyberspace is a collective responsibility among all nations and stakeholders across the world, as any implementation of cybersecurity strategy or policy rely on human resources and cybersecurity competences to mitigate and recover from cyber-related attacks.

Security and resilience of cyberspace is essential for international security and stability. However, to promote a peaceful use of ICTs and advocate for international cooperation to combat malicious activities in cyberspace, there is a need for the UN and regional and other relevant organizations to put in place joint and comprehensive capacity-building programmes to support developing states and regions to build and improve their cybersecurity capacities.

After the failure of the GGE 2017 to produce a consensual report, Meyer (2018) indicated that

The breakdown in the traditional consensual approach to UN efforts to develop a set of norms of responsible state behaviour raises alarm and uncertainty over the status of those norms and confidence building measures that have been generated by the GGE process to date.

Which means that without common understandings and approaches on international cyber-security policy, and without global cyber capacity efforts to support developing nations to build a resilient and secured cyber environment, the work done so far at international and regional levels in developing norms, rules, and confidence-building measures to prevent escalation, misperceptions, and conflicts in cyber domain may not really serve the global community. This will drastically affect international peace and security. Moreover, it is obvious that reaching the same level of cyber capabilities across regions and nations is a condition to operationalize norms of responsible states' behaviour in cyberspace and ensure international peace and security.

References

- Abdul Wahab, A. (2016). The lack of cybersecurity capacity building frameworks in Asia. *Global Forum on Cyber Expertise Magazine*. 1. Available from: www.thegfce.com/news/news/2016/06/20/the-lack-of-cybersecurity-capacity-building-frameworks-in-asia [accessed 12 June 2019].
- African Union Commission (AUC) (2017) African Union Specialized Technical Committee on Communication and Information Technologies (STC-CICT) 2nd Ordinary Session, Addis Ababa, Ethiopia, 20–24 November. Available from: <https://au.int/en/ccict2> [accessed 12 June 2019].
- African Union Commission (AUC) (2018a) Declaration on Internet Governance and Development of Africa's Digital Economy. Assembly/AU/Decl.3 (XXX). Available from: https://au.int/sites/default/files/decisions/33908-assembly_decisions_665_-_689_e.pdf [accessed 12 June 2019].
- African Union Commission (AUC) (2018b) Workshop on cyber strategies, cyber legislation and national CERTs. Available from: <https://au.int/en/cybersecurityworkshop> [accessed 12 June 2019].
- Association of Southeast Asian Nations Regional Forum (ARF) (2015) ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies (ICTs). Available from: <http://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 12 June 2019].
- Association of Southeast Asian Nations (ASEAN) (2016) ASEAN Cyber Capacity Programme. Available from: www.csa.gov.sg/~media/csa/documents/amcc/factsheet_accp.pdf [accessed 12 June 2019].
- Barmpalioi, P-N. (2016) The EU experience in global cyber capacity and institution building. *Global Cyber Expertise Magazine*. 1: 25–28.
- Basely-Walker, B. (2012) Technical and political challenges to cyber stability. Cybersecurity Conference 2012. The role of CBMs in assuring cyber stability. United Nations Institute for Disarmament Research. Available from: www.css.ethz.ch/en/services/digital-library/publications/publication.html/162492 [accessed 12 June 2019].
- Chong, Z. (2018) UN chief seeks international rules for cyberwarfare. Available from: www.cnet.com/news/un-chief-wants-international-rules-regulating-cyber-warfare/ [accessed 12 June 2019].
- Council of Europe (CoE) (2018) First African Forum on Cybercrime. Available from: www.coe.int/en/web/cybercrime/-/first-african-forum-on-cybercrime [accessed 12 June 2019].
- Council of Europe (CoE) (2019) Global Action on Cybercrime Extended (GLACY) +. Available from: www.coe.int/en/web/cybercrime/glacyplus [accessed 18 August 2018]
- Council of the European Union (EU) (2018a) Council Conclusions on Cyber Diplomacy. (11 February) Available from: www.consilium.europa.eu/register/en/content/out?&typ=ENTRY&i=ADV&DOC_ID=ST-6122-2015-INIT [accessed 12 June 2019].
- Council of the European Union (EU) (2018b) EU External Cyber Capacity Building Guidelines - Council conclusions (26 June). Available from: www.consilium.europa.eu/register/en/content/out?&typ=ENTRY&i=LD&DOC_ID=ST-10496-2018-INIT [accessed 12 June 2019].
- Council for Security Cooperation in the Asia Pacific (CSCAP) (2012) Ensuring A Safer Cyber Security Environment. Memorandum no. 20. Available from: www.cscap.org/index.php?page=memoranda [accessed 12 June 2019].
- Diplo Foundation (2017) Offensive and Defensive Cyber-Capabilities Map. Available from: <https://public.tableau.com/profile/publish/Offensivecyberdefence/Story2#1/publish-confirm> [accessed 12 June 2019].

- Diplo Foundation (2018) Diplo Briefs 2018. Available from: www.diplomacy.edu/policybriefs [accessed 12 June 2019].
- Economic Community of West African States (ECOWAS) (2017). ECOWAS and the Council of Europe join forces to help West African Countries in the fight against cybercrime. Available from: www.ecowas.int/ecowas-and-the-council-of-europe-join-forces-to-help-west-african-countries-in-the-fight-against-cybercrime/ [accessed 12 June 2019].
- European Commission (EC) (2013) *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee of the Regions (7 February, 2013).
- European Commission (EC) (2018) Operational Guidance for the EU's International Cooperation on Cyber Capacity Building. Available from: https://ec.europa.eu/europeaid/operational-guidance-eus-international-cooperation-cyber-capacity-building_en [accessed 12 June 2019].
- Gheraouti-Hélie, S. (2010). We need a cyberspace treaty. Available from: www.scarg.org/wp-content/uploads/2010/08/We-need-a-cyberspace-treaty.pdf [accessed 12 June 2019].
- Global Forum on Cyber Expertise (GFCE) (2016a) EU experience in global cyber capacity and institution building. *Global Cyber Expertise Magazine*. 1. Available from: www.thegfce.com/about/documents/publications/2016/06/01/global-cyber-expertise-magazine [accessed 12 June 2019].
- Global Forum on Cyber Expertise (GFCE) (2016b) Promoting cybersecurity due diligence across Africa. Available from: www.thegfce.com/initiatives/p/promoting-cybersecurity-due-diligence-across-africa [accessed 12 June 2019].
- Global Forum on Cyber Expertise (GFCE) (2016c) Reviewing Senegal's cybersecurity capacity maturity: a strategic approach. *Global Cyber Expertise Magazine*. 2. Available from: www.thegfce.com/about/documents/publications/2016/12/07/global-cyber-expertise-magazine-issue-2---november-2016 [accessed 12 June 2019].
- Global Forum on Cyber Expertise (GFCE) (2017) Delhi Communiqué. Available from: www.thegfce.com/delhi-communique [accessed 12 June 2019].
- Global Forum Cyber Expertise (GFCE) (2019a) About the GFCE. Available from: www.thegfce.com/about [accessed 12 June 2019].
- Global Forum on Cyber Expertise (GFCE) (2019b). Cyber Security Initiative in OAS member states. Available from: www.thegfce.com/initiatives/c/cyber-security-initiative-in-oas-member-states [accessed 12 June 2019].
- Global Forum on Cyber Expertise (GFCE) (2019c) Cybersecurity Capacity portal. Available from: www.sbs.ox.ac.uk/cybersecurity-capacity/explore/gfce [accessed 12 June 2019].
- ICT for Peace Foundation (ICT4Peace) (2016) Capacity Building Programme for International Cyber Security Negotiations. Available from: <https://ict4peace.org/activities/capacity-building/capacity-building-cs/african-union-commission-and-ict4peace-co-organized-capacity-building-for-international-cyber-security-negotiations-at-the-au-in-addis-ababa-ethiopia/> [accessed 12 June 2019].
- INFOSEC (2013) The attribution problem in cyber attacks. Available from: <https://resources.infos-ecoinstitute.com/attribution-problem-in-cyber-attacks/#gref>. [accessed 12 June 2019].
- International Telecommunication Union (ITU) (2005). World Summit on Information Society. Tunis Agenda for the Information Society. WSIS-05/TUNIS/DOC/6. Available from: www.itu.int/net/wsis/docs2/tunis/off/6rev1.html [accessed 13 June 2019].
- International Telecommunication Union (ITU) (2017) Global Cyber Security Index 2017. Available from: www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf [accessed 13 June 2019].
- International Telecommunication Union (ITU) (2018) Strengthening the role of ITU in building confidence and security in the use of information and communication technologies. Resolution 130 (REV. Dubai, 2018). Available from: www.itu.int/en/ITU-D/Cybersecurity/Documents/RES_130_rev_Dubai.pdf [accessed 13 June 2019].
- International Telecommunication Union (ITU) (2019) National CIRT. Available from: www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx [accessed 13 June 2019].
- Kerttunen, M. & Tikk, E. (2019) Strategically normative. Norms and principles in national cybersecurity strategies. European Union Institute for Strategic Studies (April). Available from: https://eucyberdirect.eu/content_research/a-normative-analysis-of-national-cybersecurity-strategies/ [accessed 12 June 2019].
- Korzak, E. (2017) The outcome of the 2016/2017 UN GGE on information security: The end of an era? Blog. East West Institute (5 September) Available from: www.eastwest.ngo/idea/outcome-20162017-un-gge-information-security-end-era [accessed 12 June 2019].

- Kurbalija, J. (2018) A tipping point for the Internet: Predictions for 2018. DiploFoundation Briefing Paper. Available from: www.diplomacy.edu/policybriefs [accessed 12 June 2019].
- Meyer, P. (2018) Global cyber security norms: A proliferation problem? ICT for Peace Foundation. Available from: <https://ict4peace.org/wp-content/uploads/2018/12/Cyber-SecNormsProlifICT4PNov2018.pdf> [accessed 12 June 2019].
- Microsoft (2019) International Cybersecurity Norms. Available from: www.microsoft.com/en-us/cybersecurity/content-hub/international-cybersecurity-norms-overview [accessed 12 June 2019].
- Organization for Security and Co-operation in Europe (OSCE) Permanent Council (2013). Initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. Decision No. 1106. Available from: www.osce.org/pc/109168 [accessed 12 June 2019].
- Organization for Security and Co-operation in Europe (OSCE) Permanent Council (2016). Confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. Decision No. 1202. Available from: www.osce.org/pc/227281 [accessed 12 June 2019].
- Organization of American States (OAS) (2004) Cybersecurity. Available from: www.sites.oas.org/cyber/EN/Pages/contacts.aspx [accessed 12 June 2019].
- Organization of American States (OAS) (2009) Consolidated List of Confidence and Security Building Measures for Reporting according to OAS Resolutions (Approved at the meeting of January 15, 2009). Available from: www.oas.org/csh/english/csbmlist.asp [accessed 12 June 2019].
- Organization of American States (OAS) (2019) CICTE: Inter-American Committee against Terrorism. Available from: www.oas.org/en/sms/cicte/default.asp [accessed 12 June 2019].
- Pawlak, P. (2014) Riding the digital wave. The impact of cyber capacity building on human development. European Union Institute for Security Studies (ISS). Available from: www.iss.europa.eu/content/riding-digital-wave-%E2%80%93-impact-cyber-capacity-building-human-development [accessed 12 June 2019].
- Pijnenburg Muller, L. (2015) Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities. NUPI Report (3). Available from: www.nupi.no/en/Publications/CRISTin-Pub/Cyber-Security-Capacity-Building-in-Developing-Countries-challenges-and-Opportunities [accessed 12 June 2019].
- Prashanth, P. (2016) Singapore unveils new ASEAN cyber initiative. *The Diplomat* (14 October). Available from: <https://thediplomat.com/2016/10/singapore-unveils-new-asean-cyber-initiative/> [accessed 12 June 2019].
- Southern African Development Community (SADC) (2018) Capacity Building Workshop on Cyber Security and SADC Regional Cyber Drill. Available from: www.sadc.int/files/2515/3719/6602/Media_Statement_SADC_Capacity_Building_Workshop_on_Cyber_Security_and_Cyber_Drill.pdf [accessed 12 June 2019].
- Subero, D. (2018) CSIRTAmericas.org – Strengthening incident response capabilities in the Americas. *Global Cyber Expertise Magazine*. 5. Available from: <http://the-gfce.instantmagazine.com/magazine/global-cyber-expertise-magazine-volume-5/csirtamericasorg/overlay/strengthening-incident-response-capabilities-in-the-americas/> [accessed 12 June 2019].
- Symantec (2016) Cybercrime and Cybersecurity Trends in Africa. Available from: www.symantec.com/content/dam/symantec/docs/reports/cyber-security-trends-report-africa-interactive-en.pdf [accessed 12 June 2019].
- Tikk, E. (2017) Voluntary, non-binding norms for responsible state behaviour in the use of information and communications technology: A commentary. UNODA Publications. Available from: www.un.org/disarmament/publications/civilsociety [accessed 12 June 2019].
- Tikk, E. & Kerttunen, M. (2018) *Parabasis. Cyber-Diplomacy in Stalemate*. Norwegian Institute of International Affairs. Report. 5. Available from: <https://nupi.brage.unit.no/nupi-xmlui/handle/11250/2569401> [accessed 12 June 2019].
- Touré, H.I. (2011) The quest for cyber peace. ITU and World Federation of Scientists. Available from: www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf [accessed 12 June 2019].
- United Nations General Assembly (UNGA) (2010) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201).
- United Nations General Assembly (UNGA) (2013) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98).

- United Nations General Assembly (UNGA) (2015a) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174).
- United Nations General Assembly (UNGA) (2015b) Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society (A/RES/70/125)
- United Nations General Assembly (UNGA) (2017) Impact of rapid technological change on the achievement of the Sustainable Development Goals (A/RES/72/242)
- United Nations Institute for Disarmament Research [UNIDIR] (2013) The Cyber Index: International Security Trends and Realities. Available from: www.unidir.org/en/publications/the-cyber-index-international-security-trends-and-realities [accessed 12 June 2019].
- Van der Meer, S. (2017) Enhancing international cyber security: A key role for diplomacy. Available at: www.clingendael.org/publication/enhancing-international-cyber-security-key-role-diplomacy

16

CHALLENGES IN BUILDING REGIONAL CAPACITIES IN CYBERSECURITY

A regional organizational reflection

Belisario Contreras and Kerry-Ann Barrett

Introduction

An age-old obligation that has been placed on regional organizations over the years has been to provide a platform for participating member states to discuss policies including security and economic measures, that impact the region. As it relates to the advent of the Internet and new technologies, these same regional bodies have now begun to consider how they can provide a vehicle to ensure the positive impact that technology can have on economic growth, competitiveness, prosperity and security, is realized. The impact of cybercrime can be a destabilizing factor for these efforts. Regional organizations therefore also have to balance the sliding scale of capacities of the individual states and global institutions to tackle new sources of vulnerabilities, on the one hand, while encouraging adoption of technology for prosperity on the other.

According to a recent blog, Chenenko, Demidov and Lukyanov (2018) stated:

A common misperception is that the principal cybersecurity threats demanding urgent international collaboration are massive, state sponsored attacks that target critical infrastructure such as power plants or electrical grids, causing massive devastation and human casualties. In fact, cyber threats are more diverse and complex, often targeting private enterprises and endangering the technical integrity of the digital world. The near-total digitalization of business models makes the global economy more vulnerable to cyberattacks, not only from states but also from criminal organizations and other non-state actors.'

With that as a present reality, what else can regional organizations do to better prepare?

Progress made

The lack of reliable information in the region has always been a challenge when considering how to strategically approach cybersecurity capacity at a national and regional level. As a consequence, the Organization of American States (OAS), through its Cybersecurity

Program at the Inter-American Committee against Terrorism (CICTE), embarked on producing research products under the umbrella of the General Secretariat, in collaboration with other regional bodies such as the OAS-IDB 2016 Cybersecurity Report, as well as the private sector (e.g. the OAS-Trend Micro Report on cyberthreats and critical infrastructure). The OAS, in essence, has consolidated itself as a clearinghouse for cybersecurity threat information and is a reference source for Latin America and the Caribbean.

As a background to why building regional cybersecurity capacity is important, Latin American and the Caribbean is the region with the third-highest Internet usage growth in the globe from 2000 to 2019: a 2,325% growth rate. In 2018, the number of smartphone users in Latin America was over 50%, compared to only 32% in 2015. This level of accessibility opens up new opportunities that can stimulate even once-dormant economies if its potential is properly harnessed. For example, Internet access generated a revenue of US\$27.65 billion in Latin America in 2016 alone, the penetration of social networks is over 70% among Internet users, and over 150 million people in the region are expected to buy goods and services online in 2019.

According to Bellasio et. al. (2018) ‘The role played by information communication technologies (ICTs) and by the networks they generate and underpin has continuously increased throughout recent decades. From an economic perspective, the potential positive impact of the Internet and ICTs on growth and development has now been widely recognized’. However, the cloak of immunity and anonymity that these technologies can provide has led to growth in illicit activities across cyberspace. How then can countries, and in particular developing nations, balance this dilemma, as despite the political, social and economic challenges the region faces, Latin America and the Caribbean are on the verge of a huge tide of opportunity to become a major hub for the Internet of Things and Smart Cities.

Regional hurdles

An open and secure Internet, in which citizens can engage and trust, is of paramount importance to the OAS. Nonetheless, one cannot ignore the ever-prevalent white elephant in the room – the risk inherent in internet use. Intolerable risks and threats without a coordinated and appropriate response without doubt diminishes the benefits a global digital market can bring.

In order to build capacity, therefore, one must identify a baseline of the challenges and existing capacities. One of our roles as a regional entity is to better understand the state of cybersecurity in the region. According to our report (OAS & Microsoft, 2018) *Critical Infrastructure Protection in Latin America and the Caribbean 2018*, jointly published with Microsoft, 48% of respondents indicated that they had cybersecurity awareness training sessions for employees, 46% indicated they had a disaster recovery plan, 42% indicated they had a cyber incident response plan, 41% indicated they had a documented cybersecurity strategy. In other words, over half of critical services providers in the region do not implement basic cybersecurity resilience practices. In another report about the *State of Cybersecurity in the Banking Sector of Latin America and the Caribbean*, 9 out of 10 banks in Latin America and the Caribbean suffered a cyber-attack last year, and 37% of the banks said they had fallen victim to at least one successful attack. The most frequent events were malicious code or malware, reported by 80% of banks, followed by violation of clear desk policies (63%), and targeted phishing (57%). One of the alarming findings in this regard was that, on average, only 41% of the banks included the conduct of a maturity assessment as part of their digital risk management strategy (OAS, 2019, p. 8). Overall, these reports indicate generally that

cybersecurity maturity and building capacity to improve maturity is not high on the agenda of several countries.

In response to this, the OAS has worked for more than a decade to strengthen the cybersecurity capacities of its 34 member states through training workshops, exercises, and awareness-raising activities which have benefited over 15,000 people since 2004. Furthermore, these capacity building efforts have resulted in the establishment of 17 Cybersecurity Incident Response Teams – including Brazil – in 11 countries. Additionally, the OAS has supported Colombia (2011 and 2016), Panama (2013), Trinidad and Tobago (2013), Jamaica (2015), Paraguay (2017), Chile (2017), Costa Rica (2017), Mexico (2017), Guatemala (2018), Dominican Republic (2018), and Brazil (2018) in the development and implementation of their national cybersecurity strategies.

Despite these advances, cybersecurity concerns need to be reprioritized at the national level with the allocation of dedicated resources to this effort. This has been particularly so in relation to the establishment of career paths for incident response professionals. For instance, many countries in Latin America and the Caribbean do not have dedicated academic programmes at the tertiary or post-graduate level focused on digital security. Another consideration is that many countries have not realized that there is a need to improve legislative frameworks which will facilitate greater cooperation among states for investigation and knowledge sharing. Revisiting legislative frameworks to include, for example, security standards and incentive schemes for new businesses and the recruitment of new talent into their economy could be a solution for a sustainable cybersecurity supply chain. For this reason, in partnership with private sector partners, OAS has been working to strengthen the cyber skills of women and youth through targeted programs throughout the region not only to develop technical expertise skills, but also to facilitate job opportunities in the cyber domain.

Aside from the policy level, another major challenge is implementation, which requires resources. Here, cybersecurity initiatives in the region often compete with national infrastructure projects (such as roads and schools) which often take precedence in national budgetary considerations. This issue of implementation also impacts the sustainability of capacity building projects which are often of a high quality but on many occasions uncoordinated and do not build on previous efforts.

Reflections from over a decade of implementing cyber capacity initiatives

There has been much global discussion on the subject of cyber capacity building. The Global Forum on Cyber Expertise, for example, was established as a global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building, with the aim of identifying successful policies, practices and ideas and multiplying these on a global level. Many nation states have entered into bilateral dialogue to advance capacity building efforts – Japan and the United Kingdom have been strengthening their cybersecurity collaboration over the last six years. In term of the development community, New America Foundation recently published *Security Digital Dividends*, in which Morgus (2018) concluded, among other points, that

integrating cybersecurity talent into the development community is necessary to equip the community with the expertise to implement cybersecurity capacity building projects on the ground and mainstream cybersecurity in their programs at a strategic level. Nonetheless, some in the development community are resigned to seeking external help via contracts.

The OAS over the years has recognized that cybersecurity preparedness enhances a country's readiness to respond to cyber threats. Furthermore, protection of a country's critical information infrastructure can be a stabilizing factor for their economy and as a consequence increases confidence in online systems and services, which could result in increased investment and uptake.

As a result, in conclusion, the following reflections can be considered to address the digital threats—digital benefits dilemma:

- Invest in human resources through core curriculum change
- Recognize that investment in sound cybersecurity practices can be a catalyst for economic growth and development
- Cooperation at the national and international level can be leveraged to build cyber capacity
- Updating legislation to address emerging threats, investigative techniques and prescribing offences for cybercrimes can be a shield to protect economic investment
- Consideration of establishing sustainable measures such as funding through the establishment of a national budget could aid in filling the gaps when the need arises
- Finally, and probably most importantly, recognizing that cybersecurity is not an abstract concept but part of domestic ecosystem will reposition it as a national priority and not just a reactionary solution.

References

- Bellasio, J., Flint, R., Ryan, N., Sondergaard, S., Gonzalez Monsalve, C., Meranto, A.S., & Knack, A. (2018) *Developing Cybersecurity Capacity: A Proof-Of-Concept Implementation Guide*. Santa Monica, RAND Corporation. Available from: www.rand.org/pubs/research_reports/RR2072.html [accessed April 26 2019]
- Chernenko, E., Demidov, O., & Lukyanov, F. (2019) *Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms*. Available from: www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms [accessed April 29 2019].
- Global Forum on Cyber Expertise (2019) Homepage – About. Available from: www.thegfce.com/about [accessed April 29 2019]
- Matsubara, M. (2019) *How can Japan-UK Cybersecurity Cooperation help ASEAN build Cybersecurity Capacity?* Available from: www.cfr.org/blog/how-can-japan-uk-cybersecurity-cooperation-help-asean-build-cybersecurity-capacity [accessed April 26 2019].
- Morgus, R. (2018) *Securing Digital Dividends, Mainstreaming Cybersecurity in International Development*. Available from: www.newamerica.org/cybersecurity-initiative/reports/securing-digital-dividends/ [accessed April 26 2019].
- Organization of American States (OAS) & IDB (2016) *Cybersecurity: Are We Ready in Latin America and the Caribbean*. Available from: <https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean> [accessed April 29 2019].
- Organization of American States (OAS) & Microsoft (2018) *Critical Infrastructure Protection in Latin America and the Caribbean 2018*. Available from: www.oas.org/es/sms/cicte/cipreport.pdf [accessed April 29 2019].
- Organization of American States (OAS) (2019) *State of Cybersecurity in the Banking Sector in Latin America and the Caribbean*. Available from: www.oas.org/es/sms/cicte/sectorbancarioeng.pdf [accessed April 25 2019].
- TrendMicro & OAS (2013) *Critical Infrastructure Protection in Latin America and the Caribbean (2013)*. Available from: www.oas.org/es/sms/cicte/cipreport.pdf [accessed April 20 2019].

SINGAPORE, ASEAN, AND INTERNATIONAL CYBERSECURITY

Benjamin Ang

Why does a small country of only 722 square kilometres, with a population of only 5.8 million (2018), spend so much of its resources on regional (ASEAN) and international cybersecurity efforts? The answer lies in Singapore's understanding of the key role that cybersecurity and international cybersecurity play in the nation's future survival and growth.

The Singapore and ASEAN approach to international cybersecurity

Cybersecurity and Singapore's Smart Nation approach

As an international centre of exchange and commerce, Singapore needs new technologies and skills to connect across the world. Domestically, almost all households have high-speed broadband Internet access and there are more phone lines than people. However, this reliance on technology also makes Singapore vulnerable to cyberattacks, as noted by Prime Minister Lee Hsien Loong in the Cybersecurity Strategy (CSA, 2016). Singapore is also a very lucrative target with reported cybercrime cases increasing from 5,351 (2017) to 6,179 (2018) (Cyber Security Agency, 2019)

Little could he have suspected that two years later, he would become a victim himself, when a patient database at Singapore Health Services Private Limited (SingHealth) was breached and personal particulars of almost 1.5 million patients were exfiltrated, of whom 159,000 (including the Prime Minister) had outpatient dispensed medication records exfiltrated.

This is not trivial in any country, and especially galling to Singapore in light of its Smart Nation initiative which aims to use technology and connectivity to empower Singaporeans to lead meaningful lives, build stronger communities, and create economic opportunities (Cyber Security Agency, 2016). The accompanying proliferation of Internet of Things devices and big data unfortunately provides an expanded threat surface. While Singapore continues to launch new initiatives, including a drowning detection system, autonomous shuttle buses, and mobile apps to access government services, on an open API-driven framework, the Minister-in-Charge of Smart Nation also acknowledged the country needs to do more to improve its security posture, particularly in the aftermath of the SingHealth data breach (Yu, 2018).

Like many other nations, Singapore is concerned about attacks on systems that run utility plants, transportation networks, hospitals, and other essential services. More uniquely,

Singapore is a banking, aviation, and maritime hub, with a significant proportion of the world's capital, traffic, and freight flowing through to its borders, and a gateway to Southeast Asia and the larger Asian Pacific region. Singapore was the third largest global foreign exchange centre and the largest in the Asia-Pacific Region in 2017. This means that disruption from data breaches, ransomware, cyber theft, and banking fraud, among others, could erode the trust that is vital to this function, and in the worst case could cripple the economy, which would in turn have negative effects on the connected global economy. No wonder then that the Commissioner for Cybersecurity called "an existential issue that undergirds and enables our future way of life" (Ghosh, 2019).

This threat continues to grow, as CSA's Director of the National Cyber Threat Analysis Centre Ho Ka Wei described in 2017 – attacks were increasing in strength and power, some as large as over one terabyte per second, and Advanced Persistent Threat (APT) attacks increased, including two at Singapore Universities in April, seeking to steal government information and research (Colquhoun, 2019).

To address these concerns, between 2015 to 2017, Singapore set up a Cyber Security Agency, created a new C4 (Command, Control, Communications, Computer) Command in the Singapore Armed Forces' (SAF) and Defence Cyber Organisation in the Ministry of Defence, and published its Cybersecurity Strategy in September 2016.

International cybersecurity in Singapore's Cybersecurity Strategy

The Cybersecurity Strategy has four pillars:

1. Building a resilient infrastructure to strengthen the critical infrastructures by working closely with private sectors and cyber security community;
2. Creating a safer cyberspace by promoting involvement from not only government but also industry and the public;
3. Developing a vibrant security ecosystem by working with industry and academia to grow the cyber security workforce; and
4. Strengthening international partnerships, especially among the ASEAN members, to address transnational cyber security issues.

Singapore's concern for international partnership is driven by the recognition that cyber threats do not respect sovereign boundaries, cyber-attackers can come from almost anywhere in the world, attackers can exploit jurisdictional gaps between countries, and cyber-attacks disrupting one country can have serious spillover effects on others, because of increasing global connectivity in trade, logistics, and financial markets.

Execution of this fourth pillar of the strategy is supposed to be through

- Forging international and ASEAN cooperation to counter cyber threats and cybercrime,
- Championing international and ASEAN cyber capacity building initiatives, and
- Facilitating exchanges on cyber norms and legislation.

On a bilateral basis, Singapore has signed Memoranda of Understanding with Australia, France, India, the Netherlands, UK, and the United States, a Joint Declaration on cybersecurity cooperation with Germany and a Memorandum of Cooperation on Cybersecurity with Japan.

The results of these efforts have propelled the republic to top ten ranking in last year's Global Cybersecurity Index (GCI), prepared by the United Nation's International Telecommunication Union (ITU) – above countries such as the United States and the United Kingdom (Singapore Business Review, 2019).

Singapore's role in ASEAN cybersecurity

Singapore carried these efforts into its chairmanship of ASEAN in 2018, playing a leading role in the region's cybersecurity agenda – investing resources in building operational, policy, and legal capacity in other member states' (through a multi-million dollar ASEAN Cyber Capacity Building Program), and building partnerships with the UN and international, multi-stakeholder initiatives like the Global Commission on Stability of Cyberspace. The annual Singapore International Cyber Week has been a useful event in convening important meetings as well as announcing initiatives, such as:

- Establishment of a Singapore-funded multi-disciplinary physical facility called the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE), which will function as a Cyber Think-Tank and Training Centre, a Computer Emergency Response Team (CERT) Centre and a Cyber Range Training Centre.
- Formation of a Singapore-UN Cyber Programme by CSA and the United Nations Office for Disarmament Affairs (UNODA) to develop and run an annual Norms Awareness Workshop and Cyber Policy Scenario Planning Workshop for representatives from ASEAN Member States.
- Most significantly for this chapter, the ASEAN Ministerial Conference on Cybersecurity (AMCC) convened at SICW 2018 agreed that Singapore would propose a mechanism to enhance ASEAN cyber coordination. This mechanism is intended to discuss cyber diplomacy, policy and operational issues.

Themes essential to international cybersecurity for Singapore and ASEAN

The abovementioned agreement by the AMCC that Singapore would propose a mechanism to enhance ASEAN cyber coordination highlights the group's willingness to chart a way forward on rules for state behaviour in cyberspace. Read together with ASEAN's renewed commitment to cyber norms, particularly the 11 norms agreed by the UNGGE in 2015, it also shows the direction the region is taking (Ang, 2018).

This shared commitment should not be taken for granted considering the disparity in cyber maturity levels among ASEAN member states, as well as the fact that only two ASEAN member states (Indonesia and Malaysia) had ever participated in earlier UNGGES (Noor, 2018).

Importance of digital economy to ASEAN

The commitment of ASEAN to international cybersecurity stems from member states' recognition that their digital economies need to be secure. At the 13th East Asia Summit (EAS) on 15 November 2018 in Singapore, Heads of State and Government of the Member States of ASEAN, Australia, the People's Republic of China, Republic of India, Japan, Republic of Korea, New Zealand, the Russian Federation and the USA, all recognized

- the importance of the ASEAN ICT Masterplan (AIM) 2020 as part of the effort to propel ASEAN toward a digitally-enabled economy that is secure, sustainable, open and transformative, which enables an innovative inclusive and integrated ASEAN Community; and
- the vital importance of ICT security for the digital economy, given that an open, secure, stable, accessible, and peaceful ICT environment is critical to connectivity and the economic development of the EAS participating countries, as well as the digital economy's increasingly important role as a driver of global economic growth, and further emphasising EAS participating countries' resolve to promote secure and resilient ICT and critical infrastructure, which can contribute to regional security and stability.

ASEAN member states' see their national security, stability and economic growth being reliant on an 'open, secure, stable, accessible, and peaceful ICT environment' for the digital economy development, not only domestically but also internationally.

Importance of rules based order to ASEAN

To achieve this goal, the same meeting noted the abovementioned ASEAN Ministerial Conference on Cybersecurity AMCC of September 2018, which

reaffirmed the importance of a rules-based cyberspace as an enabler of economic progress and betterment of living standards, and agreed in-principle that international law, voluntary and non-binding norms of State behaviour, and practical confidence building measures are essential for stability and predictability in cyberspace and in which ASEAN Member States agreed to subscribe in-principle to the 11 voluntary, nonbinding norms recommended in the UNGGE 2015 Report, as well as to focus on regional capacity-building in implementing these norms.

ASEAN had embraced the concept of the rule of law, especially at the international level, ever since its inception in 1967, and it continues to be a cornerstone of the Association until now. First recognized in ASEAN's founding document – the Bangkok Declaration – as a means to achieve regional peace and stability, the concept of the rule of law is now enshrined in the ASEAN Charter. 'The ASEAN Way has brought us to where we are now. War among the ASEAN Member States is unthinkable. And we are one of the fastest growing regions in the world today,' the Secretary-General highlighted (ASEAN 2018, 2018).

AMCC's decision to subscribe to the 11 UNGGE 2015 norms, instead of the various other sets of norms being proposed around the world, indicates that the region has made a clear choice upon which to develop policies and operations for cyberspace, out of numerous other options, some of which are compatible with ASEAN member states' values, and of some which are not. ASEAN has set a clear objective for the region to work towards, which is especially important since the UNGGE process is being reconvened. This does not preclude ASEAN member states, including Singapore, from participating in other fora, such as the Open Ended Working Group, but it does set a baseline of common understanding for ASEAN (Ang, 2018).

The importance of a rules-based cyberspace to protect nations in this region, standing upon applicable international law and the adoption of voluntary operational norms, was

underscored by Singapore's Commissioner for Cybersecurity/CE CSA David Koh, in his speech to the Atlantic Council in 2018 (Ghosh, 2019):

Cyberspace should not be any different from the physical domain.... For example, in the maritime domain, there are rules that govern how a nation-state should behave, such as through the United Nations Convention on the Law of the Sea. And similarly in the aviation domain, we abide by the rules set by the International Civil Aviation Organization. These rules underpin our modern economies and our security.... Otherwise, the alternative is a world order where might makes right, where rules and norms are routinely flouted, and where there is considerable uncertainty about the sanctity of international agreements and norms.... A small state like Singapore is like an ant in a jungle full of elephants, and we must do what we can to better secure ourselves, especially when the elephants fight.

Cynics may question the efficacy of laws like the United Nations Convention on the Law of the Sea in governing how nation-states behave, especially if said nation-states are powerful enough to ignore decisions of the Permanent Court of Arbitration. On the other hand, these exceptions may in fact illustrate how much worse the international situation could be for small states if there were no rules at all.

Public private partnership in cybersecurity in Singapore

The Heads of State at EAS 2018 also agreed that 'effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organisations'.

Several examples of active participation from the non-state sectors can be found in Singapore:

- The Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Cyber Security Agency of Singapore (CSA) signed a Memorandum of Understanding (MoU) in 2018 to advance security threat intelligence sharing and to conduct joint exercises to protect the financial services sector.
- CSA and TNB Ventures launched a Cybersecurity Industry Call for Innovation in 2018, inviting industry providers to develop innovative solutions to address specific cybersecurity challenges. The Call for Innovation was made in collaboration with five participating organizations – Ascendas-Singbridge Group, PacificLight Power, Singapore LNG Corporation, SMRT Corporation and Singapore Press Holdings.
- Most unusual for this region, Singapore launched a Government Bug Bounty programme to invite both international and local white-hat hackers to test selected, Internet-facing Government systems and identify vulnerabilities. This followed from the success of the MINDEF Bug Bounty Programme. The MINDEF Bug Bounty Programme commenced on 15 January 2018 and successfully concluded on 4 February 2018. Selected white hat hackers were invited to test eight major MINDEF Internet-facing systems for vulnerabilities, and received rewards for doing so. HackerOne, a reputable international bug bounty company, as engaged to manage the programme. A total of 264 white hats from around the world participated in this programme, including participants from Canada, Egypt, India, Ireland, Pakistan, Romania, Russia, Singapore, Sweden, and the United States. There were 100 from the local white hat community and 164 (including

57 of the top 100 ranked white hats in HackerOne's network) from HackerOne's network of about 175,000 international white hats (Lim, 2018).

There is a strong history of cooperation in cybersecurity between Singapore's public and private sectors, but the Government Bug Bounty programmes are a landmark. Since lack of cyber capacity is one of the most significant limitations that ASEAN member states face, the ability to tap into the white hat community may present a solution for states that are ready and able to embrace this option. The major caveat is a bug bounty programme requires significant investment of time and money in order to be successful; the state must prepare to handle logistics issues such as managing a sudden influx of reports, verifying that bugs are genuine, avoiding triggering false alarms, and preventing researchers from accidentally disclosing sensitive information (Ang, 2017).

Information operations and cybersecurity in ASEAN

If there is an elephant in the room for ASEAN cybersecurity, it may well be whether member states have an agreed understanding of what constitutes cyberspace with respect to state interests. Countries like the United States and Japan (and Singapore) define this domain as the technology (hardware, software) that allows free access to cyberspace, while countries like China and Russia define it as the content and interactions (speech, expression) between the users of cyberspace (Ang, 2018).

Singapore falls within the first category, as its Cybersecurity Act defines cybersecurity as

the state in which a computer or computer system is protected from unauthorised access or attack, and because of that state the computer or computer system continues to be available and operation; the integrity of the computer or computer system is maintained; and the integrity and confidentiality of information stored in, processed by or transmitted through the computer or computer system is maintained.

On the other hand, similar legislation in other ASEAN member states like Vietnam, appear to fall within the second category. Vietnam's Cybersecurity Law enacted in 2018, requires social media platforms to remove offending content within 24 hours, including propaganda against the state, as well as any 'incorrect' material that could disrupt public order or 'create difficulties' for government officials (Woollacott, 2019).

The concern over information operations in ASEAN is genuine. Campaigns of disinformation have been blamed for social unrest and violence in Indonesia and the Philippines. The borderless nature of this threat would indicate that international, or at least regional, cooperation would help.

But if ASEAN cooperation in cyberspace is to be based, as the AMCC indicates, on the UNGGE 2015 norms, then it will be necessary to limit the scope of discussion to first category (technology) issues. This would not preclude ASEAN member states from pursuing their individual strategies for managing content domestically. For example, Singapore, with its first category definition of cybersecurity, is separately passing a new law criminalizing the intentional communication of false statements of fact which could cause harm (Protection from Online Falsehoods and Manipulation Act) which is not related to its existing Cybersecurity Act. Such an approach could allow ASEAN member states to discuss cyber norms while avoiding some of the ideological disagreements that have stymied other efforts towards cooperation.

Capacity building for ASEAN cybersecurity

ASEAN also faces significant structural challenges to cooperation in cyberspace issues, stemming from the uneven distribution of technological, operational, policy, and legal capacity and capabilities of ASEAN member states. States that are struggling to get their own cybersecurity strategies, policies, and legislation in place, are not in a good position to discuss cooperation. For example, a norm that states should not allow their ICT infrastructure to be used to attack other states, is meaningless to states who yet lack the capability to secure that infrastructure in the first place.

Fortunately, substantial resources are being applied to address these challenges, such as the Singapore-initiated ASEAN Cyber Capacity Program, the Bangkok-based ASEAN-Japan Cybersecurity Capacity Building Centre, and Singapore's ASEAN-Singapore Cybersecurity of Excellence (Cyber Think Tank and Training Centre, a Computer Emergency Response Team (CERT) centre, and a Cyber Range Training Centre).

Geopolitical challenges for ASEAN cybersecurity

Finally, unlike some other regional groupings, the member states of ASEAN are not united against a common adversary. Instead, the region is a confluence point for great power competition, with China and the US asserting their roles in the region. This appears to have been manifested in cyberspace e.g. the distributed denial-of-service (DDoS) attacks on key Philippine government agencies after the Permanent Court of Arbitration ruling dismissing China's claim of ownership of the South China Sea. In another incident, Vietnamese intelligence networks were compromised, leaking sensitive information over diplomatic and military strategy, after an incident over a Chinese oil rig in Vietnamese-claimed waters in May 2014 (Piiparinen, 2016). At the same time, China and the US are both major trading partners for most ASEAN member states, and economically entangled through substantial foreign direct investments.

Mitigating measures and mechanisms in ASEAN

This chapter should end on a hopeful note. ASEAN-led mechanisms are in place such as the ASEAN Telecommunications and Information Technology Ministers' Meeting, ASEAN Ministerial Meeting on Transnational Crime, ASEAN Finance Ministers' Meeting, ASEAN Ministerial Conference on Cybersecurity and ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of ICT, the ASEAN Defence Ministers' Meeting (ADMM)-Plus Experts' Working Group Meeting on Cyber Security, the ASEAN Cyber Capacity Programme. The ASEAN Leaders' Statement on Cybersecurity Cooperation of April 2018 tasked relevant Ministers from all ASEAN Member States to recommend feasible options to better coordinate ASEAN's cybersecurity efforts and to make progress on discussions relating to the adoption of practical, voluntary norms of responsible State behaviour in cyberspace, taking reference from recommendations set out in the UNGGE 2015 Report.

The Heads of State at EAS 2018 agreed to deepen existing cooperation in the security of ICT and of the digital economy through

- Promoting an open, secure, stable, accessible, and peaceful ICT environment through effective cooperation among States, based on international law and guided by voluntary non-binding norms, rules or principles of responsible behaviour of States in the ICT

environment, including as recommended in the UNGGE Reports, while upholding States' sovereignty and protecting human rights, given that the ICT environment offers both opportunities and challenges to the international community;

- Recognising the importance of strengthening cooperation on personal data protection in order to engender trust in data management practices, including business' practices, and foster an environment that encourages data innovation;
- Supporting dialogue on how international law applies to the use of ICTs by States, as well as on norms, rules, and principles of responsible behaviour of States, confidence-building measures and capacity building as noted in UNGA Resolution A/71/28;
- Working together to provide assistance on: improving security and resilience of critical ICT infrastructure to support the demands of a robust digital economy; developing technical skills and appropriate strategies or regulatory frameworks; and bridging the divide in the security of ICTs and their use; and
- Supporting capacity-building including the development of regional approaches to capacity-building, which would be beneficial, as they could take into account specific cultural, geographic, political, economic or social aspects and allow a tailored approach, and the development and use of e-learning, training and awareness-raising with respect to ICT security.

They also agreed to cooperate in non-technological ways such as:

- Promoting sustainable economic growth and prosperity and address the digital divide and development gap, by supporting digital economy initiatives including in: investment and innovation, entrepreneurship, assisting Micro, Small and Medium Enterprises (MSMEs) to utilise ICTs and participate in the digital economy, developing a digital-ready workforce, raising awareness of security in the use of ICTs, promoting regional integration into the global marketplace, and building synergies to complement the ASEAN Smart Cities Network Initiative; and
- Fostering cooperation to support a secure and resilient digital infrastructure, and effective information exchange within the region.

References

- Ang, Benjamin (2017) 'Why Mindef's move to engage white hat hackers may pay off'. *TODAYonline*, 21 December. Available from: www.todayonline.com/commentary/why-mindef-s-move-engage-white-hat-hackers-may-pay [accessed 25 April 2019].
- Ang, Benjamin (2018) 'Next steps for cyber norms in ASEAN'. *S. Rajaratnam School of International Studies*, October. Available from: www.rsis.edu.sg/rsis-publication/cens/next-steps-for-cyber-norms-in-asean [accessed 25 April 2019].
- ASEAN 2018 (2018) "East Asia summit leaders' statement on deepening cooperation in the security of information and communications technologies and of the digital economy." *ASEAN Singapore 2018*. Available from: www.asean2018.sg/Newsroom/Press-Releases/Press-Release-Details/EAS_InformationCommunication [accessed 25 May 2019].
- Colquhoun, Lachlan (2019) "Heightened danger in Singapore as cyber attacks increase." *Telecom Asia*. Available from: www.telecomasia.net/content/heightened-danger-singapore-cyber-attacks-increase [accessed 20 June 2019].
- Cyber Security Agency (CSA) (2016) "CSA | Singapore's cyber security strategy." *Cyber Security Agency*. Available from: www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy [accessed 20 June 2019].
- Cyber Security Agency (2019) "CSA | Singapore cyber landscape 2018." *Cyber Security Agency*. Available from: www.csa.gov.sg/news/publications/singapore-cyber-landscape-2018 [accessed 20 June 2019].

- Ghosh, Nirmal (2019) "Singapore's cyber security chief says international norms, partnerships are key issues." *The Straits Times*, 23 April. Available from: www.straitstimes.com/singapore/singapores-cyber-security-chief-says-international-norms-partnerships-are-key-issues [accessed 25 April 2019].
- Lim, Min Zhang (2018) "Hackers find 35 bugs in first Mindef bug bounty programme, \$19,500 paid out." *The Straits Times*, 21 February. Available from: www.straitstimes.com/singapore/hackers-find-35-bugs-in-first-mindef-bug-bounty-programme-19500-paid-out [accessed 25 February 2019].
- Noor, Elina (2018) "ASEAN takes a bold cybersecurity step." *The Diplomat*, 4 October. Available from: thediplomat.com/2018/10/asean-takes-a-bold-cybersecurity-step/ [accessed 25 February 2019].
- Piiparinen, A. (2016) "China's secret weapon in the South China Sea: Cyber attacks." *The Diplomat*, 22 July. Available from: <https://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/> [accessed 3 March 2019].
- Singapore Business Review (2019) "Singapore ranks 10th in global cybersecurity: Study." *Singapore Business Review*. Available from: sbr.com.sg/information-technology/news/singapore-ranks-10th-in-global-cybersecurity-study [accessed 9 February 2019].
- Woollacott, Emma (2019) "Days after introduction of 'cybersecurity' law, Vietnam has Facebook in its sights." *Forbes Magazine*, 9 January. Available from: www.forbes.com/sites/emma-woollacott/2019/01/09/days-after-introduction-of-cybersecurity-law-vietnam-has-facebook-in-its-sights/#5d32695e26c5 [accessed 9 February 2019].
- Yu, Eileen (2018) "Singapore touts open platforms in smart nation drive, acknowledges need to do better in security." *ZDNet*, 9 October. Available from: www.zdnet.com/article/singapore-touts-open-platforms-in-smart-nation-drive-acknowledges-need-to-do-better-in-security/ [accessed 9 February 2019].

18

SUB-REGIONAL VIEWS ON INTERNATIONAL CYBERSECURITY

CLMV countries

Lim Ratha and Sok Kunvath

Cambodia, Laos, Myanmar and Vietnam are the last four countries to enter into the Association of South East Asian Nations (ASEAN). ASEAN attaches great importance to assisting its new members hasten economic integration and reduce regional disparities. To help boost the four nations, within the cooperative endeavours of the CLMV countries, human resources and capacity development and information communication technologies (ICT) were identified as the priority areas for narrowing the regional divide (ASEAN, 2012). Improved skills and connectivity will not only hasten knowledge transfer, but it will also assist in the alleviation of poverty. Moreover, national ICT and cybersecurity prowess is needed to counter cybercrime that deprives countries of the financial resources needed for societal and economic development. Falling short on the promise of sustainable development may lead to social disturbances and local and regional unrest.

In the following chapter, we analyze the four countries' cyber-security status. In the International Telecommunication Union 2017, *Global Cybersecurity Index*, against the 'pillars' of legal, technical, organizational, capacity building and cooperation measures, the Lao People's Republic is rank 76th best of the CLMV nations; Cambodia, Myanmar, Vietnam are fairly close being assessed 91st, 99th and 100th, respectively among 164 ranking positions (ITU, 2017). More importantly, the CLMV countries' ICT development offers insights into national and sub-regional concerns that need to be addressed in the ASEAN, but also in global, negotiations.

Cambodia

Cambodia, a new emerging market among lower middle-income economies in the region, has enjoyed its growing middle class of young active populations who are open to new trends of culture and technology, in particular the use of cyberspace in this digital era. The government, acquainted of the situation, has developed its Industrial Development Policy 2015–2025, with an emphasis on ICT as a driving factor towards the realization of its shift from an agricultural to an industrial based economy (World Bank Group, 2018: Konrad Adenauer Stiftung, 2018). To ensure the safety of the use of ICT in reaching its goals, the government has laid out the framework for the nation to defend against cyber-crime.

Currently, the Ministry of Posts and Telecommunications (MPTC) is the leading national cybersecurity institution. The Ministry of Interior (MOI) works on cybercrime, whereas the Ministry of Foreign Affairs and International Cooperation (MFAIC) performs cyber diplomacy and matters related to cybersecurity at the ASEAN Regional Forum (ARF). Under the MPTC, there is the Information and Communications Technology Security Department that houses Cambodia's Computer Emergency Response Team (CamCERT) (Australian Strategic Policy Institute, 2017) whose missions include awareness and outreach, quality assurance and digital forensics, standard and risk, and digital authentication, within public key infrastructures. One of the roles of CamCERT is incident reporting, where public and private individuals can report any security breach that they have encountered and, in turn, they will receive technical assistance from CamCERT to help them mitigate the issues. Incident coordination, security advisory and tips and alerts are also among the services that CamCERT offers (Cambodia Computer Emergency Response Team, 2017). On the flip side, CamCERT is not part of the Asia-Pacific CERT (APCERT) group unlike Laos, Myanmar, and Vietnam.

As of today, Cambodia has not yet passed a cybercrime law. On the other hand, the Criminal Code that went into force on December 2010 and the 2015 Telecommunications Law, containing provisions on handling cybercrimes, are available legislative instruments. Moreover, a Sub Decree on 'Digital Signature', approved in December 2017, will become one more component to improve security in the cyber world. The government has also laid out the framework for the enhancement of cybersecurity, namely the ICT Masterplan 2020, where the government introduced measures and initiatives to further improve its cybersecurity capacity (KOICA, 2014). In addition to this Masterplan, the Telecom-ICT Development Policy 2020, which was adopted in April 2016, is another instrument to boost cybersecurity initiatives in Cambodia.

To further enhance its capacity, Cambodia has implemented several further activities including: Cambodia Cyber Angkor, a cyber exercise for government CIOs across all government ministries and related parties; Cambodia Cyber Challenge (CCC) targeting young talents, mostly university students, to show their cyber capability locally, but also regionally through Singapore Cyber Conquest and ASEAN Cyber Sea Game, and the Stay Safe Online Cambodia awareness campaign. In addition, Cambodia also took part at ASEAN-JAPAN Cybersecurity Capacity Building Center as well as ASEAN Cyber Capacity Program (ACCP) from Singapore. Cambodia participated regularly in ASEAN Cyber Drill (ACID) and ASEAN-JAPAN Cyber Exercise. The nation also improves its incident response framework through the establishment of CSIRT-Network that provides trainings for its officials and private sectors (Ou, 2018a).

Cambodia has made progress in developing their cybersecurity. However, the nation still has multiple challenges that it needs to address in order to further bolster its cyber-security system. As laid out in the ICT Masterplan 2020, to further develop the nation's cybersecurity, Cambodia needs to address its limitations, including: outdated cybersecurity infrastructure; a lack of laws and regulations as well as policies, standards, and norms; and the need to raise public awareness on the subject matter. According to the Director of ICT department, MPTC, Mr. Ou Phannarith, one thing that is common for most developing countries is the priority of budget allocation. Physical infrastructure is still the critical sector that the government needs to heavily focus on, and invest in, since it also answers to the demands of the people. A very limited budget is by far the most challenging problem hindering the development of a robust and resilient cybersecurity infrastructure. An essential element, which not only Cambodia is lacking but most ASEAN members are struggling to deal with, is the development and management of the needed human resources in the field of cybersecurity (Ou, 2018b).

Laos

Before 2012, Laos was the only country in ASEAN where there was no National Computer Incident Response Team (Lao Computer Emergency Response Team, 2017). With more than 2.4 million internet users in the country, together with the growth of the ICT sector, it is critical for Laos to bolster its cybersecurity to thwart attempts by cyber-criminals in attacking or operating in the country.

The Ministry of Posts and Telecommunications is the primary governing cybersecurity institution. The Ministry sets the direction of Lao ICT industries along with producing yearly and five-year plans. Lao Computer Emergency Response Team (LaoCERT) is under the supervision of this ministry. Being the national CERT of Laos, it is continuing to develop its capacity and competences in cooperation with other CERTs organizations in the region. Incident handling, cyber security protection, security information dissemination, and awareness raising are some of the responsibilities of LaoCERT. In 2018, Lao PR's statistics of incident response show that 43% were Bad IP, 33% were Web Defacement, 21% were Malware and 3% were Phishing Sites (Sounnalat, 2018).

The policies and laws to promote cybersecurity in the country – such as the National ICT Policy issued in 2009, the 2011 Telecommunication Law in 2011, the 2012 E-Transaction Law and the Criminal Law, the 2015 Cyber Crime Law, and the 2017 Data Protection Law – show slow but steady process in creating the necessary legislative and administrative frameworks. All contain essential provisions to enhance, safeguard, and promote national cybersecurity (Australian Strategic Policy Institute, 2017).

When it comes to regional cooperation, LaoCERT has been a member of the Asia Pacific CERT since October 2014. The aim of APCERT is to support the creation of a safe, clean, and reliable cyberspace in the Asia Pacific Region. LaoCERT also joined ASEAN-Japan Activities in 2012 and has signed cooperative agreements with other CERTs organizations such as ThaiCERT in 2013, IDSIRT in 2015, and VNCERT and CNCERT in 2017. Based on the annual report of the APCERT, in 2017 alone Laos has participated in 11 training courses, conducted three drills and exercises, and attended 12 seminars and conferences on cybersecurity that highlighted the government's commitment in bolstering the nation's cybersecurity (Asia Pacific Computer Emergency Response Team, 2017).

In six years, Laos has transformed itself from having no National Computer Incident Response Team into having its very own LaoCERT, established institutions to take charge in cybersecurity governance, created legislations to govern its cybersecurity, and participated in regional cooperation. Despite its achievements, Laos is similar to its neighbouring countries. The country lacks cybersecurity experts in the field and the implementation process of the legislation is still limited. It does not have a National Cyber Security Strategy which would set forth goals and measures to improve its current capacity and to effectively provide a safe ICT environment for its users and combat against cybercrime and other threats and risk. Laos needs a sustainable budget for supporting ICT infrastructures, international cyber cooperation, and to establish roles and responsibilities to further improve the current cybersecurity situation of the nation (Sounnalat, 2018).

Myanmar

Having been isolated from the world during the military regime, post-2014 Myanmar experienced a sudden surge of digitalization. In 2011, in a population of 50 million, there were only 130,000 internet users in Myanmar, a figure that has now risen to 14 million

(Thaung & Kyaw, 2017). Thus, the question arises as to what has Myanmar installed or prepared to secure the information of those users from cyber threats?

The Ministry of Communications and Technology is Myanmar's prime ICT and cybersecurity institution. Within the ministry, the Information Technology and Cyber-Security Department has the main responsibility to maintain and develop the field. Part of the Department, the National Cyber-Security Center (NCSC), houses Myanmar's Computer Emergency Response Team (mmCERT) tasked with cybersecurity incident handling. In addition to incident handling, mmCERT also works to increase public awareness, provides technical advisory supports, and shares the latest threats and security news with the public (Ministry of Communications and Technology, 2018).

Drafting Myanmar's cyber legislation is the first priority of the Information Technology and Cyber-Security Department. There are, however, three ICT-related laws that govern Myanmar's Information Communication and Technology: the 1996 Computer Science Development Law; the 2004 Electronics Transaction Law; and the 2013 Telecommunications Law (Achard, 2018).

Beyond the domestic development of cybersecurity frameworks and mechanisms, Myanmar has also participated in discussions on cybersecurity as a member of ASEAN and TSUBAME under APCERT. The country has also extended cooperation with Singapore to develop its military cyber capabilities and participated in training through the Myanmar-Singapore Training Compendium. Myanmar has also cooperated with Japan to develop its cyber policy. With the CLMV framework cybersecurity policy, international law and voluntary norms as well as operational links and capabilities are being discussed (Australian Strategic Policy Institute, 2017).

Myanmar has a long way to go to improve its cybersecurity capacity. The nation has so far engaged in the foundational, technical capacity building, but wider legal and political frameworks need to be developed to set and govern national cybersecurity measures. For example, Myanmar needs to define the unclear roles and responsibilities between the NCSC and the Cyber Crime Units. Myanmar, similarly to her partners, has to live with very limited financial and human resources and undeveloped cybersecurity awareness among the population (Ministry of Communications and Technology, 2018). Another problem identified by the World Bank is that the cyber infrastructure is based on mobile broadband access rather than fixed broadband. The inevitably slower speeds increase the vulnerability to DDoS (Distributed Denial-of-Service) attacks, which occur when multiple systems flood the bandwidth of a system. The dependency on the mobile infrastructure also undermines the ability to employ more advanced and effective technologies (Lars & Niels, 2018). As ICT is one of the (few) engines that spur a country's development, it is important that the government has and allocates more resources to the development of national information infrastructure and services, cybersecurity included, from the security perspective.

Vietnam

Vietnam, despite being a one-party, formerly socialist state, has undergone some tremendous digitalization in its economy, politics, and society. More than half of the population are Internet users and Vietnam has shown a relatively strong effort to utilize the benefits of digitalization.

In Vietnam, there is a clear division of roles between the ministries when it comes to cyber-security. More precisely, three ministries have been given the role of governing Vietnam's cyber-security: the Ministry of Information and Communications is in charge

of national cybersecurity (civil affairs); the Ministry of Public Security is in charge of combating cybercrime; and the Ministry of Defense is in charge of cyber defence. There are three additional institutions that are housed by the Ministry of Information and Communications: the Vietnam Computer Emergency Response Team (VNCERT); the Authority of Information Security (AIS); and the National Electronic Authentication Center (NEAC). Of these three sub-units, VNCERT works exclusively with incident coordination (Authority of Information Security, 2017).

The legislation in place to provide measures to secure the cyber-environment include the 2001 Management and Use of Internet Services Decree, the 2005 Law on E-Transactions, the 2006 Law on Information Technology, the 2009 Telecommunication Law, and the 2015 Law on Cyber-Information Safety (Australian Strategic Policy Institute, 2017). From the beginning of 2019, the Law on Cyber-Security, adopted in June 2018, will come into force. This will further contain the provisions to control the content in the information networks (Vietnam Business Law, 2018).

From 2015 to 2016 the number VNCERT processed incidents rose from ca. 19,000 to over 130,000, the majority of them being defacement, malware, and phishing. VNCERT also organized or participated in workshops and the above-mentioned training courses, exercises, and drills to enhance its incident detection, analysis, and handling capacity. It regularly collaborates with other CERTs in the regions, e.g. Chinese, Japanese, Korean and Lao computer emergency response teams. VNCERT has also organized regional and sub-regional training events and workshops such as the ‘Senior Level Workshop on International Cyber Security Policy and Diplomacy for CLMV Countries’, and ‘The 2nd CAMP Regional Forum’.

Vietnam continues to strengthen its cyber-security capacity as highlighted through its organizational structure, emerging legislation, and the daily activities of VNCERT. Currently, following the introduction of the new cyber law, Vietnam is facing a crucial business challenge. The new cyber law promoted by the security ministry to protect the country from threats of tens of thousands of cyber-attacks that could cause economic losses and threaten the social order, means technology companies are less likely to invest in Vietnam as the law requires them to set up local offices and store the data locally (Vietnam Business Law, 2018).

Conclusion: ASEAN and beyond

Looking at the full picture of ASEAN, the member-states have clearly stressed the importance of enhancing national and regional cybersecurity as well as recognising the value of developing a set of practical cybersecurity norms of behaviour in ASEAN. At the ASEAN Ministerial Conference on Cybersecurity (AMCC) in Singapore in September 2018, it was agreed that Singapore would propose a mechanism to enhance ASEAN cyber coordination that is intended to cover cyber diplomacy, policy, and operational issues. The AMCC also agreed to subscribe in principle to the 11 voluntary, non-binding norms recommended at the 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), referred as the 11 UN GGE 2015 norms. These recommendations, among others, include: not knowingly allowing one’s territory to be used for internationally wrongful acts using ICTs; not conducting or knowingly supporting ICT activity contrary to international law that damages critical infrastructure; responding to requests made by another State who is subjected to malicious ICT acts; taking steps to ensure the integrity of the supply chain; and responsible reporting of ICT vulnerabilities (Benjamin, 2018). The AMCC’s

present decision that Singapore should devise a framework for cooperation in ASEAN and the reiteration of the 11 UN GGE 2015 norms, instead of any other set of norms being proposed, indicates that the region has made a clear choice to subscribe to global cyberspace frameworks. How well these ambitions and normative frameworks suit ASEAN and ASEAN member state values requires careful elaboration. As a way forward for ASEAN, the new direction that the organization is taking is a promising move and a clear pathway for what the organization needs to do to enhance cybersecurity in the region. Yet, for Singapore to develop a framework for ASEAN as a whole effectively, the differences in levels of cyber maturity between CLMV and the other six members, policy priorities and levels of development and resources are the issues that needed to be taken into account.

Nonetheless, looking further at the four Southeast Asian countries, they are still in the early stage of their development, with each of the countries focusing on their own cybersecurity capacity building, which is one of the challenges that ASEAN faces. Their engagement is also focused more at the regional rather than international level, especially centring on ASEAN and its dialogue partners.

The CLMV countries are struggling with similar issues – the lacks of resources, technical expertise, and personnel in the field of cybersecurity that undermine their safety against cyber-attacks, as well as their capacity to perform more than capacity building. As a way forward for the CLMV countries, the four nations should start off by tackling the challenges that they currently face – only when domestic cyber-security is secured can the four nations look to engage more in the international arena.

Although international cybersecurity is more than the sum of national cybersecurity, the CLMV experience stresses the need to develop foundational ICT capabilities to create secure technical and favourable societal and economic conditions. Cambodia, Lao PR, Myanmar, and Vietnam, in fact, represent fairly well the average nations for whom the superpower-centric and arms control-dominated international cybersecurity dialogue is relevant but still rather alien. Financing, legal and administrative frameworks, infrastructure, work force competence, and an overall domestic culture of cybersecurity cannot be achieved by focussing on strategic stability between the cyber superpower nations or on *jus in bello*. We hope that through the story of the CLMV we are able to shape international cyber and information security negotiations towards more sustainable concepts of peace, stability and development.

References

- Achard, D. (2018) *Cybercrime Situation*. Available from: <https://rm.coe.int/03-myanmar-presentation/168072bd20> [accessed 15 December 2018].
- Ang, B. (2018) *ASEAN's Response to Cybersecurity*. Available from: www.khmertimeskh.com/50544824/aseans-response-to-cybersecurity/ [accessed 10 January 2019].
- ASEAN (October, 2012) *The ASEAN-Japan Plan of Action*. Available from: https://asean.org/?static_post=the-asean-japan-plan-of-action-2 [accessed 18 December 2018].
- Asia Pacific Computer Emergency Response Team (2017) *APCERT Annual Report 2017*. Available from: www.apcert.org/documents/pdf/APCERT_Annual_Report_2017.pdf [accessed 4 December 2018].
- Australian Strategic Policy Institute (2017) *Cyber Maturity in the Asia-Pacific Region 2017*. Available from: www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/ASPI%20Cyber%20Maturity%202017_AccPDF_FA_opt.pdf [accessed 18 December 2018].
- Authority of Information Security (2017) *Overview of Cyber Security in Vietnam*. [Presentation] Authority of Information Security.

- Cambodia Computer Emergency Response Team (2017) *About CamCERT: What We Do*. Available from: www.camcert.gov.kh/en/what-we-do/ [accessed 5 December 2018].
- International Telecommunication Union (ITU) (2017) *Global Cybersecurity Index*.
- KOICA (2014) *Cambodian ICT Master Plan 2020*. Available from: www.trc.gov.kh/wp-content/uploads/2016/10/Cambodian-ICT-Masterplan-2020-요약본영문.pdf [accessed 10 December 2018].
- Konrad Adenauer Stiftung (2018) *Economic Transformation in Cambodia and Abroad, Digital Insights*.
- Lao Computer Emergency Response Team (2017) *About LaoCERT*. Available from: www.laocert.gov.la/en/Page-1- [accessed 17 December 2018].
- Lars, G. & Niels, S. (2018) *Cyber Security Capacity Building in Myanmar*. Available from: <https://brage.bibsys.no/xmlui/bitstream/handle/11250/2498132/NUPI%2bPolicy%2bBrief%2bMyanmar.pdf?sequence=2&isAllowed=y> [accessed 9 January 2019].
- Ministry of Communications and Technology (2018) *Cyber Security Status in Myanmar*. [Presentation] Tokyo, 16–17 December.
- Ou, P. (2018a) *Building Tomorrow Cyber's Workforce: Cambodia Experiences*. [Presentation] Tokyo, 16–17 December.
- Ou, P. (2018b) Director of the Information Communication Technology Department. (Personal communication, 11 December 2018).
- Sounnalat, K. (2018) *Current Status on Cyber Security Policy in Lao PDR, 2018*. [Presentation] Ministry of Post and Telecommunications, 2018.
- Thaung, H. & Kyaw, N. (2017) *Cybercrime Situation in Myanmar*. Available from: www.doj.gov.ph/files/OOC/OOC%20-%20TOT/Cybercrime%20Situation%20in%20Myanmar.pdf [accessed 14 December 2018].
- Vietnam Business Law (July, 2018) *Vietnam's New Cyber Security Law 2018*. Available from: <https://vietnam-business-law.info/blog/2018/7/30/vietnams-new-cybersecurity-law> [accessed 20 December 2018].
- World Bank Group (July 2018) *Benefiting from the Digital Economy, Cambodia Policy Note*. [accessed 9 January 2019].

REGIONAL CYBERSECURITY APPROACHES IN AFRICA AND LATIN AMERICA

Lucy Purdon and Francisco Vera

Introduction

As the international cybersecurity debate searches for new directions, more attention should be paid to regional approaches to cybersecurity. There has been a flurry of activity in Africa and Latin America over the past few years, resulting in a number of cybersecurity strategies, policies and legislation that demonstrate differing government attitudes towards security and human rights, both positive and negative.

Regional approaches are not necessarily grounded in international security concerns. Equally, international policies cannot be realized until these national and regional approaches are taken into consideration and either accepted or challenged. Whilst peace and security may be a claimed goal, many governments view developing cybersecurity policy and legislation as an opportunity to shore up their own power, without putting much effort into analysing the risks, threats, and beneficiaries of their work.

In particular, focusing on criminalising and monitoring online behaviour and increasing state surveillance powers rather than addressing the root problems of insecure systems can leave a country unprepared for what may come and vulnerable to attacks and data breaches, which can be catastrophic for people's privacy and security.

Ultimately, international cybersecurity is only as strong as its weakest link, so it is in the interest of the international community to pay attention to regional approaches and have a better understanding on the particular challenges that they are facing.

This chapter also takes a look at the influence on the Africa and Latin America's cybersecurity approaches by bodies like the European Union, the Council of Europe, and countries like China, Russia, and the United States.

As Internet penetration grows outside more developed countries, new challenges and trends will necessarily emerge, and the current international cybersecurity agenda will become more diversified and complex. Whilst this is not an exhaustive analysis of all the elements involved, we hope that this chapter will provide readers with a good idea of the current state of cybersecurity policy and legal trends in Africa and Latin America and serve as an opportunity to foster a critical reflection on what the global cybersecurity challenges are when it comes to developing policy and legislation.

Approaches to cybersecurity in Africa

African States on the whole follow their own individual paths when it comes to developing cybersecurity and cybercrime legislation. But it did not start out this way. In the early part of the twenty-first century, there were efforts towards a regional approach to cybersecurity in Africa, mostly led by the development of several model laws that intended to harmonize cybercrime legislation across the region.

The legacy of these model laws is that, in general, the focus in Africa is heavily weighted towards tackling cybercrime. This is worrying as it leaves actual cybersecurity, essentially a technical approach to securing systems such as critical infrastructure and consumer services from attack and failure, largely under resourced. Governments often fail to draw the distinction between cybersecurity and cybercrime, use the term interchangeably and often lump both issues together in one law. But addressing cybersecurity and cybercrime is complex. It requires separate consideration of the issues and safeguards designed to address the unique privacy and security implications of each.

Since 2010, Privacy International is aware of cybersecurity and/or cybercrime laws being adopted or drafted in the following 13 countries in Africa: Egypt, Ethiopia, Kenya, Malawi, Mauritius, Morocco, Nigeria, Senegal, South Africa, Tanzania, Tunisia, Uganda, and Zimbabwe. The worst proposed simply increasingly extends the list of crimes to include criminalization of legitimate expression online and attempts to justify intrusive state surveillance rather than securing systems against attacks (Privacy International, 2018).

Progress has also been marred more recently by an ultimate lack of strong regional leadership and policy cohesion, along with political instability. In 2017 and 2018, Presidents were forced to resign in both South Africa and Zimbabwe. Kenya went through another tense Presidential election in 2017, which was annulled and rerun among claims of hacked voter systems. Zimbabwe held historic elections in July 2018, marred by violence and claims of vote rigging. In this context, other parties with particular strategic interests, namely China, have played a significant role in shaping Africa's approach to cybersecurity, with the USA and Europe increasingly taking a back seat.

Early 2000s competing regional approaches

Early regional approaches in Africa focused on the creation of model cybercrime laws. For example, in 2008 the International Telecommunications Union (ITU) in collaboration with the European Union (EU), launched the Harmonisation of the ICT Policies in Sub-Saharan Africa ('HIPSSA') project. This was following a request by economic organizations and regulators in Africa for assistance in harmonising laws, and a framework of reference formally adopted by ICT ministers from African Union Member States (ITU, 2008).

That effort led to the development of the Southern African Development Community (SADC) Model Law on Cybercrime Model Law on Computer Crime and Cybercrime. SADC Member States were then encouraged to implement this in their respective jurisdictions, thereby bringing about the regional harmonization of cyber laws.

One of the main criticisms from civil society is that language in the SADC Model Law has paved the way for the criminalization of legitimate freedom of expression online, particularly criticism of the government, by including a vague provision on harassment by means of electronic communication, conflating cybersecurity with restrictive control of the online space.

In 2013, SADC and the ITU sent two missions to Zimbabwe to help incorporate the Model Law into national law. The eventual result was the draft *Cybercrime and Cybersecurity Bill* (Zimbabwe, 2017). Civil society has repeatedly expressed concern that offences on cyber bullying, harassment and transmission of false data messages, which are very similar to section 22 of the SADC Model Law, will result in the stifling of freedom of expression and unlawful interference with privacy of communications online. As the Media Institute of Southern Africa (MISA) outlined in a briefing, ‘the government is giving the impression of wanting to shield itself from criticism rather than protect the people from actual harm’ (MISA, 2018).

These are not over-reactions and Zimbabwe’s civil society have cause for concern, as reflected in other laws. Tanzania’s 2015 Cybercrime Act also follows the SADC Model Law closely, including provisions on harassment and the ‘publication of false information’ in Section 16. One of the first applications of the Act, and indeed Section 16, was the arrest of 36 members of the Legal and Human Rights Centre (LHRC), an NGO in Tanzania which had been critical of the Act, for compiling election observations (Dar Post, 2015).

Under the same Section 16, a man was sentenced to three years (Dar Post, 2016) in prison for calling President Magufuli an ‘idiot’ on Facebook. Section 16 has been used to arrest political opposition, teachers and students accused of insulting the President via social media.

The Council of Europe (CoE) was particularly scathing about HIPSSA and the SADC Model Law in a 2014 report, concluding that, ‘apart from being generally fraught with failed attempts at innovation, poor language and drafting, technically and legally incorrect and overreaching provisions, HIPSSA’s provisions and drafting is unsafe’ (Council of Europe, 2014).

It is perhaps not a surprise that the CoE was so critical of the HIPSSA project and SADC Model Law, as they are keen for their own Convention on Cybercrime 2001 (known as the ‘Budapest Convention’) to be the gold standard that succeeds in harmonising cybercrime laws in Africa and beyond. By 2011, no African States had ratified it, leading to a plea by the Council of Europe for African States to do so.

In 2017, the Economic Community of West African States (ECOWAS) and the CoE jointly organized a conference intended to promote the Budapest Convention and encourage African States to join. As of June 2018, Mauritius, Morocco and Senegal had ratified the Budapest Convention.

Looking for a leading regional approach

In 2014 the African Union (AU) adopted the *African Convention on Cybersecurity and Personal Data Protection* as an attempt to re-centre a regional approach, but this too has not been widely ratified by States. As of May 2018, only Mauritius and Senegal had ratified it, out of 55 States. But Mauritius and Senegal have also ratified the Budapest Convention, which leaves us no closer to knowing which the leading regional approach is.

While the Budapest Convention is not widely ratified in Africa, it is easy to get the impression that parts of it have been ‘copied and pasted’ into national legislation. The CoE estimates that 45 States globally unofficially draw on the Budapest Convention for legislation, including 13 in Africa (Lucchetti, 2018). The problem here is that the importance of human rights protections is often lost.

When international treaties’ provisions are copied and pasted into national legislations, the context and many important obligations to the parties of a treaty (States) tend to be lost. For example, Article 15 of the Budapest Convention is clear that adequate protection

for human rights must be provided for. This is clear in the context of being a CoE Member State, as CoE Member States are all parties to the European Convention on Human Rights which offers strong protection on human rights backed up by legally binding judgments of the European Court of Human Rights. Such protection is absent for non-CoE states which ratify the Budapest Convention.

When the Budapest Convention is ratified, or sections copied and pasted by non-member States, without accompanying effective human rights safeguards, what is left is legislation that includes very privacy intrusive measures.

This is echoed in civil society concerns the addition of new investigative powers granted to law enforcement to investigate cybercrime in model laws and regional approaches, which make their way into domestic cybercrime laws without appropriate safeguards. One of the countries that embodies this concern and appears to be one of the 45 States which drew from the CoE's Budapest Convention is Kenya, which passed its *Computer Misuse and Crimes Act* in May 2018.

Part IV of the Act not only grants new investigative powers such as real time collection of traffic data and interception of content, but extends them to police officers. This is a huge leap in Kenya's surveillance regime, essentially hidden in a cybercrime law with little scrutiny or debate.

Under Kenya's existing surveillance legislation, the National Intelligence Services Act 2012 only permits the Director General of the National Intelligence Service (NIS) the ability to intercept an individual's communications subject to prior application to the High Court for a warrant. The Prevention of Terrorism Act 2012, grants police officers above the rank of a Chief Inspector the power to request an interception of communications order from the High Court. By giving the power of collection and interception to police officers, the Computer Misuse and Crimes Act is clearly expanding the Kenyan's surveillance regime.

The human rights' path to harmonization

The introduction of several competing model laws and regional approaches was ultimately not conducive to a harmonized regional approach in Africa. It resulted in States cherry picking aspects of different model laws to implement in their own national legislation, sidelining human rights protections and safeguards in the process, which has opened the door for expanding surveillance regimes and restrictive control of the online space.

National civil society organizations have stepped up and tried to fill the gap of human rights safeguards by making concrete suggestions not just at the national level, but also the regional. While the right to privacy is not expressly featured in the African Charter on Human and People's Rights, a recognition of the right to privacy at regional level would potentially be a huge step forward in developing good cybersecurity frameworks placing people and their rights at the centre.

At the 62nd session of the African Commission on Human and People's Rights (ACHPR) in April 2018, civil society took the opportunity to present salient privacy issues and advocate for stronger privacy protections across Africa.

At the NGO Forum, which preceded the main ACHPR session, Privacy International, the Legal Resource Centre (LRC), the International Network of Civil Liberties Organisations (INCLO) and the Centre for Intellectual Property and Information Technology Law (CIPIT) at Strathmore University in Kenya proposed recommendations for an ACHPR's resolution on the right to privacy in a statement which was successfully adopted by the NGO Forum, calling for the ACHPR to formally recognize privacy as a fundamental right which

must be protected and promoted in Africa. The statement, presented by LRC, called on the ACHPR to resolve:

That human dignity, as contained in Art. 5 of the African Charter on Human and People's Rights is the core right and value which underpins the need for the respect, recognition and promotion of the right to privacy of all people in Africa

and

that the mandate of the Special Rapporteur on Freedom of Expression and Access to Information include privacy concerns where these impinge on the ability to communicate and receive opinions freely.

Alongside this initiative, a group of civil society organizations are leading a process to revise the Declaration of Principles on Freedom of Expression in Africa to include privacy issues and digital rights (IFEX, 2018). Unfortunately, the AU appears to be more interested in limiting civil society participation rather than encouraging it. At the AU summit in June 2018, the Executive Council adopted the Decision EX.CL/Dec.1015(XXIII), which appears to limit the independence of the ACHPR, particularly the capacity to decide which NGOs could be granted observer status. If civil society are to meaningfully contribute to regional advances, they need a regional human rights body that is able to fulfil its protection mandate effectively and independently.

With the regional approaches either fizzling out or being weakened from the inside, another actor has taken centre stage in assisting African nations with both regulatory inspiration and providing technology – China.

The influence of China on cybersecurity in Africa

At home, China's own 2017 cybersecurity law reflects China's ongoing ambitions for both control of the Internet and dominance of the domestic cybersecurity market. China of course has the money and population to sustain a totally home-grown cybersecurity industry and exercise a level of 'Internet sovereignty' that other authoritarian countries could only dream of. But any country can pass a restrictive law and purchase surveillance technology in the name of cybersecurity. And China is on hand to help in Africa, both by inspiring legislation and by supplying surveillance technology.

China's investment in Africa over the years is well known, including the 2013 Belt and Road Initiative. In 2015, Tanzania was selected as a pilot country for the Initiative (Ministry of Commerce of the People's Republic of China, 2017). The Cyberspace Administration of China (CAC), which oversees Internet censorship in China, reportedly provided some technical advice (Yi, 2017) regarding placing restrictions on Internet content and blogging activity, similar to China's own content controls, which is now reflected in Tanzania's own 2015 cybercrime law. There are also echoes of China's approach to data localization in the legislation of Belt and Road Initiative partners such as Egypt and Nigeria.

Africa is a massive potential market for Chinese technology – from cheap smartphones and devices to CCTV. An increased focus on cybercrime means an increased demand for investigative tools, and China is keen to supply the latest surveillance must-haves.

Most recently, Zimbabwe signed a deal with Chinese company CloudWalk for a country wide facial recognition surveillance system. Facial recognition is already big business in

China, and has reportedly been trialled in the Xinjiang province, referred to as a ‘real life laboratory for surveillance’, as millions of ethnically Uyghur and Kazakh Muslims are under constant surveillance (Hawkins, 2018).

Approaches to cybersecurity in Latin America

The first approach to cybersecurity in Latin America was through approving cybercrime laws. In 1993 Chile passed the first cybercrime law of the region, heavily inspired by France’s 88–19 Law (Moscoso, 2014). By year 2000, also Bolivia, Paraguay, El Salvador, Mexico, and Peru, also had their own cybercrime laws.

After its creation in 1948, and between the decades of 1950–1990, a traditional conception of national security dominated the agenda of the Organisation of American States (OAS), which in the context of the Cold War and strong influence from the United States of America, gave way to the infamous ‘national security doctrine’, used in the region to justify the violent seizure of power and the emergence of dictatorships all over the region, and serving as the rationale to focus in the ‘internal enemy’ and allow for the commission of serious human rights violations against people who fell in that category (Álvarez and Vera, 2016).

From 1990, conceptions of security in the Latin America started to change. From a traditional concept of national security to a new paradigm of multidimensional security, materialized in the adoption of the ‘Declaration on Security in the Americas’ by the OAS (OAS, 2003).

Within this paradigm of multidimensional security, came the first sign of a regional approach to cybersecurity in Latin America. In 2014, during the 34th ordinary session of the OAS, a resolution titled ‘The Inter-American Integral Strategy to Combat Threats to Cybersecurity’ (OAS, 2004) was adopted. Such resolution did not provide a concept of cybersecurity, but it was built on the need for a ‘comprehensive strategy for protecting information infrastructures that adopts an integral, international, and multidisciplinary approach’.

The strategy provided clear mandates to different existing parts of the OAS to carry on coordination and capacity building activities. The Inter-American Committee against Terrorism (CICTE) stayed in charge of the formation of an Inter-American alert, watch, and warning network to rapidly disseminate cybersecurity information and respond to crises, incidents, and threats to computer security. The Inter-American Telecommunication Commission (CITEL), on the other hand, is in charge of the identification and adoption of technical standards for a secure Internet architecture. Finally, the Group of Governmental Experts on Cyber-crime of the Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA), was tasked with ensuring that OAS Member States have the legal tools necessary to protect Internet users and information networks.

As civil society in the region has noted (Fundación Karisma, ADC and Tedic, 2018), those different mandates have been carried out in very diverse ways: whilst CITEL and REMJA have complied with their assignments with limited reach and stakeholder engagement, the CICTE has created programmes to build, train and engage national CSIRTs; and over time it has also engaged with other stakeholders, including policymakers, through simulation exercises and technical assistance on the creation of national cybersecurity strategies (CICTE, 2013).

As for other organs of the OAS involved on cybersecurity, the Inter American Commission on Human Rights has been increasingly playing a role, by monitoring and publishing reports on Internet and human rights (IACHR, 2013 and 2016).

Cyber norms development in the region

On norms development in the region, it is possible to identify two separate initiatives: one at a sub-regional level in South America, and the other at the Inter-American level, under the auspices of the OAS.

At a South American level, the attempt to develop norms came from the Union of South American Nations (UNASUR), and specifically in their South American Security Council (Artigo 19, 2017). After Snowden's revelations of mass surveillance conducted by intelligence agencies from the United States, United Kingdom and others, Brazil pushed for the creation of a working group on cyber defence within the South American Security Council.

Their stated goals were promising: develop confidence building measures (CBMs), creating secure channels of communication and carrying forward general cooperation on the issue of cyber defence. However, outside from some meetings, this working group did not produce the expected results, and in the current context where the UNASUR is losing regional influence, it isn't likely to produce any in the foreseeable future.

At the Inter-American level, the Committee on Hemispheric Security of the OAS is a specific body that works as an advisor, mediator and expert in security and defence issues, and they are in charge of keeping a record of Confidence Building Measures in the region. It also contributes with the implementation of the Inter-American Integral Strategy to Combat Threats to Cybersecurity. In fact, it provided the necessary boost for the adoption of such resolution (Fundación Karisma, ADC, TEDIC, 2018, p. 32)

On 7 April, 2017, the Member States of the CICTE decided to establish a

Working Group on Cooperation and Confidence-Building Measures in Cyberspace in charge of preparing a set of draft confidence-building measures (CBMs), based on the consensus reports of the United Nations Group of Governmental Experts (UN GGE) to enhance interstate cooperation, transparency, predictability and stability and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs, and report its advances and activities to the Inter-American Committee against Terrorism (CICTE) and the Committee on Hemispheric Security of the OAS.

(CICTE, 2017)

Later, in February 2018, the Working Group held a meeting and proposed a first set of two measures consisting on sharing cybersecurity policies and designating a contact point in each country. The measures were approved by the member states of the CICTE on 4 May, 2018, along with the continuation of the working group.

Those two measures are still very basic, and they are nowhere near the OSCE developments on the field, but the region have great opportunities on this field, given its lack of armed conflicts and its positioning as a 'peaceful region'.

National CERT and cybersecurity strategy development

Outside of joint OAS resolutions and strategies, one of the main areas in which this regional approach has been expressed is the creation of a regional network of national Computer Emergency Response Teams (CERTs), and the preparation of national cybersecurity strategies. The CICTE has had a key role across these processes, providing their technical support and assistance throughout them.

The CICTE's approach has also evolved with time, in line with new technical and policy demands from OAS members. At first, it offered mostly capacity building on how to build technical response teams. Then, it started facilitating cybersecurity strategy development, not only in regard to their content but also by bringing diverse stakeholders into the discussion (CICTE, 2018)

One such example of this evolution is Colombia, where after the creation of the national CERT (ColCERT), the CICTE conducted trainings and roundtables that led to the first cybersecurity strategy in the region. This strategy was reflected in a planning document named CONPES 3701, also known as 'Policy guidelines for cybersecurity and cyberdefence'.

This planning placed the Ministry of Defence at the centre of the policy development – this, however, could not prevent several state surveillance scandals (Fundación Karisma, ADC, TEDIC, 2018), and the policies contained in the planning reflected an overly securitized approach to cybersecurity.

In 2015, before the end of the CONPES 3701's timeline, and to overcome its limitations, the Colombian Government asked the OAS to send a technical assistance mission to assess the state of digital security in the country, which was integrated by experts from countries, industry and international bodies such as the OECD.

After this mission, a new cybersecurity strategy was adopted in 2016, the CONPES 3854, with its main focus shifting from the militarization of the cyberspace to promoting economic and social development and ruled by four principles: Safeguarding human rights and fundamental values, adopting an inclusive approach, shared responsibility, and adopting a risk-based approach. Whilst this new approach constitutes a positive development, the process of elaboration of the CONPES (and the principles) lacked meaningful participation from civil society, and the measures privileged an economic development approach over the social aspects of cybersecurity (Fundación Karisma, ADC, TEDIC, 2018, p. 25).

In parallel, the CICTE has also provided technical assistance to countries such as Dominican Republic, Paraguay, Mexico, Costa Rica and Panama, all of them based on capacity building and stakeholder consultations, giving an increased importance to the latter as the CICTE methodology has evolved, going from limited consultations in the beginning, to a more inclusive approach (Schnidrig, Shears & Kaspar, 2018).

Even countries that did not receive direct assistance from the CICTE through formal missions and capacity building activities, like Chile, received resources and informal support to conduct their processes from them, which helped the country to develop their strategies in line with regional and global trends.

One thing that stands out in the Chilean cybersecurity, is their language in relation with both human rights and encryption. Instead of focusing on cybercrime or the general legal framework, like most cybersecurity policies or strategies in the region, this policy was centred on a different outcome: protect people's rights in cyberspace, encompassing crime prevention, trust building and fundamental rights, with specific references to the rights to freedom of expression, privacy, and due process. Further, it contained specific commitments to foster encryption and against intentional vulnerabilities or backdoor mechanisms, like the following:

Measures based on this policy shall promote encryption adoption for online users according to international standards, and under no circumstances the intentional use of unsafe technologies shall be promoted, or there will be and obligation by any person or organisation to provide digital services to implement 'back door' mechanisms compromising or increasing any risks associated with the security technologies used.

(Chilean National Cybersecurity Policy, 2017, p. 13)

Another way in which the CICTE has been contributing to a regional approach to cybersecurity, is through partnering with the private sector to conduct trainings and research in the region, giving way to several publications that range from good practices guides to cybersecurity assessments (Fundación Karisma, ADC, TEDIC, 2018).

There are some challenges that can arise from such partnerships, however. The first is to preserve a neutral image before its beneficiaries, given the fact that many of those companies provide products and services to Latin American countries. The second, is to partner with other entities from governments, academia and civil society from the region, in order to diversify their content production.

However, and despite the availability of support from the CICTE, countries like Argentina, Brazil and Peru (among others) are still lagging behind on their cybersecurity policy development, putting into question how effective this regional approach can be when there is not enough support from national governments.

Another shortcoming of the cybersecurity policy development is the lack of enforcement of these strategies and policies at the national level, given the very formalistic legal traditions in Latin America, which makes it difficult to collaborate between different state actors when there are not clear legal mandates.

This creates the risk of having cybersecurity policies that focus more on grand statements and posturing rather than managing and reducing security risks in the cyberspace, including violation of fundamental rights, such as privacy. Government attempts to disproportionately increase surveillance in Chile, such as the attempt to approve a decree increasing data retention times and affect the use of encryption, is a good manifestation of such contradictions (Viollier, 2018).

Cybercrime in the region

As it happens in Africa, one major influence when it comes to cybercrime legislation is the Budapest Convention and the work of the Council of Europe to help its promotion. Over the last 5 years, countries in the region started to sign and ratify the Budapest Convention (Dominican Republic, Chile, Argentina, Costa Rica, Panamá and Paraguay have ratified the treaty by 2018), and some have been trying to adapt it to their legislations even without formally ratifying it, like Perú (Morachimo, 2014). On the other hand, countries like Brazil have showed opposition to the Convention (UNODC, 2015).

Some countries have used cybercrime legislation to criminalize behaviours which should not be considered a criminal offence, including in some cases criminalising the legitimate exercise of human rights protected by human rights instruments.

The role of the REMJA, one of the organs of the OAS, has been to provide technical assistance on cybercrime to Governments, but in doing so they have failed to involve and consult with stakeholders outside of government, including civil society. Their reports also show the push for some measures that are at odds with human rights, in particular the right to privacy, such as promoting the adoption of data retention schemes (REMJA, 2014).

Foreign influence in the region

The major cybersecurity foreign influence in the region is still the US, through the OAS and bilateral cooperation on security and defence. Neither Russia or China have had particular influence on cybersecurity in the region outside their traditional areas of influence (mostly Cuba and Venezuela).

However, many countries in the region have been acquiring surveillance tools from European countries such as the United Kingdom and Italy, which have been the source of public scandals due to their sophistication and abuses. Another country that is becoming increasingly influential in Latin America is Israel, which on top of selling surveillance technologies that have given way to surveillance scandals like what happened with the hacking of Mexican activists using software from the company NSO, have also been establishing policy cooperation on cybersecurity issues with Latin American countries such as Chile.

Conclusion

Probably due to its huge language, cultural and economic diversity, Africa's approach to cybersecurity is not a global one, or even regional. It is perhaps an inevitability that, when presented with a variety of 'model laws', States will cherry pick the parts that appeal to them and go their own way. Unfortunately, these cherry-picked parts are usually the most repressive, and States fail to underpin legislation with human rights protection and safeguards.

The two main problems to tackle in the region are the disproportionate focus on cyber-crime legislations and the desire to increase control of the online space and surveillance. Actual cybersecurity concerns, technically securing systems, take a back seat. By focusing on control and restrictions rather than securing systems, African nations are potentially leaving themselves vulnerable. Global cybersecurity is, after all, only as strong as the weakest link.

The lack of strong regional leadership has allowed other regional and national influences to step in. Top-down solutions such as model laws or specific treaties such as the AU Convention on Cybersecurity and Personal Data Protection haven't been effective so far, with African countries not even signing or ratifying the latter.

China's influence is concerning, given their own restrictive cybersecurity laws and willingness to supply very invasive technology without adequate safeguards. Civil society organizations are seeking to address these shortcomings in the cybersecurity policy developments in Africa, but face significant challenges at domestic and regional level.

In Latin America, on the other hand, the regional emphasis has been on building technical response teams and capacity building, instead of specific treaties. By building institutional capacity, the region has been able to evolve their approach to cybersecurity issues and being less centred on cybercrime issues. This process hasn't been exempted from foreign influence though. The OAS itself is perceived by many as a tool to help United States influence, and they still play a large role in the region (Shaw, 2014).

When it comes to cybercrime, Latin America face similar challenges with Africa on how to adopt a legislation that protects people instead of ramping up State powers, with deficient adaptations of the Budapest Convention, followed by vague definitions of crimes that pave the way to repressing dissent.

Regions should develop their own voices in the global cybersecurity discussions, with a focus on their particular challenges, which could have a positive impact on international peace and security, bringing more diversity and closeness to discussions that tend to become overly abstract.

Paying more attention to these regional approaches to cybersecurity is also a great learning opportunity for the global community, creating room for innovative policy solutions that could be more successful in protecting people, devices, and networks, improving their lives instead of restricting them in the name of security.

References

- African Union (2014) Convention on Cybersecurity and Personal Data Protection. Available from: www.au.int/web/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf [accessed 12 January 2019].
- African Union (2018) Personal Data Protection Guidelines for Africa. Available from: https://au.int/sites/default/files/newsevents/workingdocuments/34421-wd-aucprivacyguidelines_2018508_en-1.pdf [accessed 12 January 2019].
- Álvarez, D. & Vera, F. (2016) Cybersecurity and Human Rights in Latin America. In: *Towards an Internet Free of Censorship II*. Available from: www.palermo.edu/cele/pdf/investigaciones/Towards_an_Internet_Free_of_Censorship_II_10-03_FINAL.pdf [accessed 12 January 2019].
- Artigo 19 (2016) Desenvolvimento de políticas de cibersegurança e ciberdefesa na América do Sul - Estudo de caso sobre a atuação governamental brasileira. Available from: <http://artigo19.org/blog/2016/03/10/da-ciberseguranca-a-ciberguerra-o-desenvolvimento-de-politicas-de-vigilancia-no-brasil/> [accessed 12 January 2019].
- Biegon, J. (2018) The rise and rise of political backlash: African Union Executive Council's decision to review the mandate and working methods of the African Commission. Available from: www.ejiltalk.org/the-rise-and-rise-of-political-backlash-african-union-executive-councils-decision-to-review-the-mandate-and-working-methods-of-the-african-commission/ [accessed 12 January 2019].
- Breland, A. (2017) How white engineers built racist code – and why it's dangerous for black people. Available from: www.theguardian.com/technology/2017/dec/04/racist-facial-recognition-white-coders-black-people-police [accessed 12 January 2019].
- Chilean National Cybersecurity Policy (2017). Available from: www.ciberseguridad.gob.cl/media/2017/04/NCSP-ENG.pdf [accessed 12 January 2019].
- CICTE (2017) Establishment of a working group on cooperation and confidence-building measures in cyberspace. CICTE/RES.1/17
- CICTE (2018) Regional confidence-building measures (cbms) to promote cooperation and trust in cyberspace. CICTE/RES.1/18
- Council of Europe (2014) Cybercrime model laws. Discussion paper prepared for the Cybercrime Convention Committee (T-CY). Available from: <https://rm.coe.int/1680303ee1> [accessed 12 January 2019].
- Council of Europe (2018) List of Budapest Convention signatories. Available from: www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=to7zo4Qj [accessed 12 January 2019].
- Cybersecurity Law of the People's Republic of China (2017). Available from: www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ [accessed 12 January 2019].
- Dar Post (2015) EU, US: cybercrime law stomping on rights. Available from: www.darpost.com/2015/11/eu-us-cybercrime-law-stomping-on-rights/ [accessed 12 January 2019].
- Dar Post (2016) Presidential insult leads to cybercrime charge. Available from: www.darpost.com/2016/04/presidential-insult-leads-to-cybercrime-charge/ [accessed 29 October 2019].
- Fundación Karisma, ADC, TEDIC (2018) El rol de organizaciones multilaterales en la agenda latinoamericana de seguridad digital: El caso de la OEA. Available from: <https://adcdigital.org.ar/wp-content/uploads/2018/06/DDHH-y-Seguridad-Digital-2.pdf> [accessed 12 January 2019].
- Hawkins, A. (2018) Beijing's big brother tech needs African faces. Available from: <https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/> [accessed 12 January 2019].
- Hayduk, D. (2016) Presidential insult leads to cybercrime charge. Available from: www.darpost.com/2016/04/presidential-insult-leads-to-cybercrime-charge/ [accessed 12 January 2019].
- Hove, K. (2018) The continental context behind the development of Zimbabwe's ICT laws. Available from: www.ctldfrica.org/2018/07/15/the-continental-context-behind-the-development-of-zimbabwes-ict-laws/ [accessed 12 January 2019].
- Inter American Commission of Human Rights (IACHR) (2013) Freedom of Expression and Internet Report. Available from: www.oas.org/en/iachr/expression/docs/reports/internet/foe_and_internet_report_2013.pdf [accessed 12 January 2019].
- Inter American Commission of Human Rights (IACHR) (2016) Standards for a free, open and inclusive internet. Available at: www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf [accessed 29 October 2019].

- International Telecommunications Union (ITU) (2008) Support for harmonization of the ICT Policies in Sub-Saharan Africa. Available from: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx [accessed 12 January 2019].
- ITU (2013) Southern African Development Community (SADC) Model Law. Available from: [www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC Model Law Cybercrime.pdf](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf) [accessed 12 January 2019].
- ITU Support for harmonization of the ICT Policies in Sub-Saharan Africa. Available from: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx [accessed 12 January 2019].
- Joplin, T. (2018) China's newest global export? Policing dissidents. Available from: www.albawaba.com/news/china%E2%80%99s-newest-global-export-policing-dissidents-1139230 [accessed 12 January 2019].
- Kenya computer misuse act (2018). Available from: kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf [accessed 13 January 2019].
- Kirkpatrick, D. & Ahmed, A. (2018) Hacking a prince, an emir and a journalist to impress a client. Available from: www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html [accessed 12 January 2019].
- Lucchetti, M. (2018) Cybercrime legislation in Africa, Regional and International standards. Available from: https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-05.pres_cybercrime_legislation_in_africa_12apr2018_matteo_l.pdf [accessed 12 January 2019].
- Mbuvi, D. (2011) African States Urged to Ratify Budapest Cybercrime Convention. Available from: www.csoonline.com/article/2129762/data-protection/african-states-urged-to-ratify-budapest-cybercrime-convention.html [accessed 12 January 2019].
- Media Rights Agenda (2018) African NGOs to revise Declaration of Principles on Freedom of Expression. Available from: www.ifex.org/africa/2018/06/11/declaration-free-expression/ [accessed 13 January 2019].
- Ministry of Commerce of the People's Republic of China (2017) The Belt and Road Initiative and China-Tanzania Relations. Available from: <http://english.mofcom.gov.cn/article/newsrelease/counseloroffice/westernasiaandaficareport/201705/20170502573605.shtml> [accessed 12 January 2019].
- MISA (2018) Trudging down the wrong path: A policy brief on the Cyber crime Bill. Available from: <http://zimbabwe.misa.org/2018/04/07/trudging-wrong-path-policy-brief-cyber-crime-bill/> [accessed 12 January 2019].
- Morachimo, M. (2014) ¿En qué quedó la ley de delitos informáticos? Available from: <https://hiperderecho.org/2014/01/en-que-quedo-la-ley-de-delitos-informaticos/> [accessed 12 January 2019].
- Moscoso, R. (2014) The Act 19.223 in general and the hacking crime in particular. *Revista Chilena de Derecho y Tecnología*. 3: 1.
- Ngwanakilala, F. (2017) Tanzania orders arrest of opposition MP for insulting president. Available from: www.reuters.com/article/us-tanzania-politics/tanzania-orders-arrest-of-opposition-mp-for-insulting-president-idUSKBN19P1JJ [accessed 12 January 2019].
- OAS (2003) Declaration on security in the Americas. Available at: www.oas.org/en/sms/docs/declaration%20security%20americas%20rev%201%20-%2028%20oct%202003%20ce00339.pdf [accessed 29th October 2019]
- OAS (2004) AG/RES. (XXXIV-O/04) A comprehensive inter-American cybersecurity strategy: A multidimensional and multidisciplinary approach to creating a culture of cybersecurity. Available from: <https://ccdcoc.org/sites/default/files/documents/OAS-040608-InterAmericanCyberSecurityStrategy.pdf> [accessed 12 January 2019].
- OAS (2018) Cybersecurity Program description. Available from: www.sites.oas.org/cyber/en/pages/default.aspx [accessed 12 January 2019].
- OAS (2013) Inter-American Committee Against Terrorism. Report on activities. Available from: www.oas.org/es/sms/cicte/documents/sesiones/2013/report%20on%20activities%20of%20cicte%20cicte00820s03.pdf [accessed 12 January 2019].
- Phillips, T. (2018) China testing facial-recognition surveillance system in Xinjiang. Available from: www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report [accessed 12 January 2019].
- Privacy International (2017) Track, Capture, kill: Inside communications surveillance and counter-terrorism in Kenya. Available from: https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf [accessed 12 January 2019].

- Privacy International (2018a) Lone voices leading the way: How civil society in Africa is successfully countering government narratives on cyber security. Available from: <https://privacyinternational.org/blog/2160/lone-voices-leading-way-how-civil-society-africa-successfully-countering-government> [accessed 12 January 2019].
- Privacy International (2018b). Teach 'em to phish: State sponsors of surveillance. Available from: <https://privacyinternational.org/sites/default/files/2018-07/Teach-em-to-Phish-report.pdf> [accessed 12 January 2019].
- REMJA (2014) Report on 2014 meeting. Available from: www.oas.org/juridico/english/cyber_experts.htm [accessed 12 January 2019].
- Santiago Times* (2018) Chile announces cybersecurity alliance with Israel. Available from: <https://santiagotimes.cl/2018/09/24/chile-announces-cybersecurity-alliance-with-israel/> [accessed 12 January 2019].
- Schmidrig, D., Shears, M., & Kaspar, L. (2018) Multistakeholder approaches to national cybersecurity strategy development. Available from: www.gp-digital.org/publication/multistakeholder-approaches-to-national-cybersecurity-strategy-development/ [accessed 12 January 2019].
- Shaw, C. M. (2004) *Cooperation, Conflict and Consensus in the Organisation of American States*. New York: Palgrave.
- Snow, J. (2018) Amazon's face recognition falsely matched 28 members of congress with mugshots. Available from: www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [accessed 13 January 2019].
- Tanzanian Cybercrimes Act (2015). Available from: https://rsf.org/sites/default/files/the_cyber_crime_act_2015.pdf [accessed 14 January 2019].
- Temperini, M. (2013) Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. Available from: <http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf> [accessed 12 January 2019].
- UNODC (2015) Non-paper submitted by Brazil reflecting its views on the issue of cybercrime. Available from: www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_24/ECN152015_CRP5_e_V1503408.pdf [accessed 12 January 2019].
- Viollier, P. (2018) Por una ley de delitos informáticos que proteja y respete los derechos de las ciudadanas en internet. Available from: www.derechosdigitales.org/12581/la-ley-de-delitos-informaticos-en-chile/ [accessed 12 January 2019].
- Williams, G. (2018) Why China will win the global race for complete AI dominance. Available from: www.wired.co.uk/article/why-china-will-win-the-global-battle-for-ai-dominance [accessed 15 January 2019].
- Yi, Y. (2017) Tanzanian, Chinese media experts meet over opportunities, challenges. Available at: www.xinhuanet.com/english/2017-07/26/c_136472133.htm [accessed 29 October 2019].
- Zimbabwe draft Cyber Crime and Cyber Security Bill (2017). Available from: www.ictministry.gov.zw/sites/default/files/downloads/cybercrime%20and%20cybersecurity%20bill%202017%20%20third%20draft.%20with%20cn%27s%20additions%20printed%20for%20chairman%20%26%20minister%20dd%209%20june%202017%20-%20mictpcs%20comments-4.pdf [accessed 29 October 2019].

A REGIONAL VIEW ON INTERNATIONAL CYBERSECURITY

The scope, problem, and remedies as seen
in West Africa

Folake Olagunju Oyelola

Introduction

The Economic Community of West African States (ECOWAS) is a diverse geographical region made up of a combination of 15 coastal, landlocked, and island countries. The region has experienced growth in access to the Internet attributable to an increase in mobile Internet penetration (GSMA, 2018) and the improvement in the expansion of infrastructure, policy and regulatory harmonization of the ICT sector. Access to various submarine cables has made connectivity to the world-wide network possible with most of the coastal countries connected to at least one submarine cable whilst the landlocked countries have at least two routes to submarine cables through coastal countries. Meanwhile, the region has adopted common policies and regulations to attract more investment and enable a faster development of the sector in order to achieve the digital transformation of the region.

According to Roller and Waverman (2001), there is evidence of a significant positive causal link between the development of infrastructure and economic growth, especially when a critical mass of telecommunications infrastructure is developed. The improvement of the broadband infrastructure through various submarine cables and terrestrial fibre optic as well as the adoption of ICTs has created unprecedented opportunities to accelerate social and economic development and at the same time exposed the vulnerabilities within the West African landscape (GFCE, 2016). Schia (2018) observed that the establishment of the requisite institutions, regulations, and other mechanisms required to manage the introduction of new technology in the global south is often not on a par with the technology itself. The paucity of these mechanisms along with human resource capacity deficiencies are contributing factors to the vulnerabilities being experienced within the region and have exacerbated the cybersecurity and cybercrime challenges.

Challenges

Cybercrime is an international problem that requires cross jurisdictional collaboration across all national boundaries to successfully address it. Though late adopters of technology, in recent years, Africa as a whole has seen an upsurge in the rates of cybercrime (Serianu, 2016);

the belief is that some perpetrators of cyber-enabled mass marketing frauds originate from West Africa, particularly Nigeria (Whitty, 2018). However, it must be noted that perpetrators in domains such as Europe, Ukraine, and USA also mask themselves as West Africans. In addition, the protocol of free movement in West Africa (ECOWAS, 1979) that allows for movement and settlement of many of these individuals in other West African countries has aided the spread of various forms of malfeasance, including cybercrimes, throughout the region. Considering the ubiquitous nature of ICTs as an integral part of society, the notion of being *cyber-secure* is gaining strides within West Africa.

The approach of the region to handling cybersecurity is quite nebulous, given that is a region where most of the countries are classified as least developed, with the priority of governments being placed on socioeconomic development and bridging the digital divide. Within West Africa, the connectedness of information systems is not as inter-related and interconnected as other parts of the world. This is also evident from the global cybersecurity index (ITU, 2017) where most countries are classified as making commitments whilst a few are seen as being already involved in cybersecurity initiatives. Interestingly, though, this non-contiguous nature, though in itself limiting in exploiting the power and opportunity of a connected society, acts as a natural defence of this nascent society, much like isolated local area networks within the global Internet.

Regionally, the decision was made in the early 2000s by the regional economic community that cybersecurity be taken seriously, thus a set of regional legal instruments were later adopted on electronic transactions, personal data protection, and on fighting cybercrime in order to not only secure online transactions and protect personal data of West African citizens but also to respond to cybercrime. The act concerning electronic transactions defines the rules to regulate these activities, notably the obligations and responsibilities of actors, as well as measures to secure electronic transactions in the ECOWAS space whilst the act on personal data protection aims at establishing a mechanism in each member state to protect privacy.

Despite the existence of these instruments, the region is under great pressure to tackle the challenges imposed by the borderless nature of cyberspace from the users' perspective, and to achieve some semblance of cybersecurity. This is particularly challenging due to inadequate implementation of adopted legal and regulatory frameworks, as delays have been experienced in the adaptation of national legislations to regional legal instruments, despite provisions imposing a time limit of two years for the domestication of regional texts. In addition, some provisions within these instruments are sometimes not enacted or improperly implemented. For instance, while the provision in the data protection act requests all countries to setup a national data protection authority, to date only a few countries have complied. Untimely compliance by countries to their obligations under the provisions of the regional acts prevents the assurance of timely regional harmonization and uncertain cross border cooperation within the ECOWAS.

At the continental level and following the initiatives taken in West Africa, the African Union adopted the African Union Convention on Cyber Security and Personal Data Protection (the 'Malabo Convention') in 2014 which aims to address the need for harmonized legislations necessary to enhance cooperation in the area of cyber security in its countries. To enter into force, the convention needs to be ratified by at least 15 African countries and regrettably after four years after its adoption the convention is still yet to enter into force. On the international front, the ratification of the Convention on Cybercrime of the Council of Europe (Budapest), a treaty with a focus on cybercrime and electronic evidence, also remains a challenge. In a bid to facilitate legislation reform in African countries, Jamil (2016) highlights

that the Malabo Convention without being complemented by the Budapest Convention cannot be used as a means of harmonizing cybercrime domestic laws and enabling cooperation amongst countries as it does not contain the stipulated provisions that can enable such whilst the Budapest convention provides a mechanism for international cooperation.

Accession and ratification of both conventions are important within the region as these can facilitate information sharing and provision of technical assistance between countries. As Cole et al. (2008) have highlighted, initiatives in Africa are primarily focused on cybercrime legislation. The ultimate goal is to create a single digital market in West Africa and there can be no single digital market without a secure cyber environment in the region. However, due to the porous nature of the region, legislation is only part of the solution – a culture of cybersecurity and good cyber-hygiene needs to be cultivated. In view of this, governments and regional bodies have the responsibility to ensure the creation of an enabling environment which tackles other challenges such as poor awareness, limited financial resources, and a lack of human expertise.

Like ICT, cybersecurity is a cross cutting issue and needs to be addressed in a holistic approach to better secure the West African cyberspace. Cole et al. (2008) states that Africa has other persistent problems such as poverty, famine, and HIV AIDS to contend with other than cybersecurity. This is all the more true, since most of the countries within the region are classified as being among the least developed countries and devote meagre budgetary allocations to cybersecurity. At the same time, the impacts of an insecure cyber space are underestimated by most countries even though cyber-attacks can affect their security and economy. The security of a nation and the wellbeing of its people are paramount to its development, hence the connectedness between priority areas and cybersecurity needs to be established for resource mobilization.

The region's vulnerability has led to reported losses of millions of dollars for individual countries (Serianu, 2016). The vulnerability of the region is expected to continue to rise as cyber threats become more complex and sophisticated. In addition, the liberalization of the ICT sector has led to the development of broadband networks including mobile broadband as well as innovative services and applications that will increase vulnerability of networks and devices.

Ways forward

The susceptibility of the region, coupled with the limited information available in the region, led to the adoption of a regional cybersecurity agenda. The agenda is an overarching initiative that aims to support countries in strengthening their cybersecurity capabilities to better respond to cyber threats, ensure enhanced protection of the national and regional infrastructure, serve national priorities, and maximize socio-economic benefits as well as to build confidence and security in the use of ICTs. This coordinated approach and shared responsibility is required to minimize the impact cybercrimes have on the region. A coordinated approach and shared responsibility by both the private sector and government is required to minimize the impact cybercrimes have on the region, as government cannot do it all and indeed most of the primary infrastructure from undersea cables, service providers and end user devices are all privately owned.

Awareness is a good starting point in cultivating a culture of cybersecurity in the region. According to Bada, Von Solms and Agrafiotis (2018) the opportunity exists to ride on the efforts being made by African countries to increase ICT literacy by combining ICT development with cybersecurity awareness. Enduring cybersecurity awareness can be established by

getting political buy-in, key leader engagement, and a commitment to improve the security of the cyberspace from key stakeholders in government. The utilization of a multi stakeholder approach and involvement is paramount to the success and sustainability of cybersecurity awareness campaigns.

Capacity building within the region needs a more inclusive approach with emphasis on south-south cooperation to tackle the dearth of expertise within the region. Emphasis should be placed on capacity building of stakeholders, the capability to handle cybercrime, enact appropriate legislation, cyber resilience and strengthen international cooperation. All these actions can be encompassed in a structured cybersecurity strategy that is implemented in a coordinated manner with a cross section of relevant stakeholders including the public and private sector. Effort is required from countries to adopt and implement such a strategy if it does not exist.

According to Serrano (2015), effective critical infrastructure protection includes the ability to identify threats to and reduce the vulnerability of such infrastructures to damage or attack, minimize damage and recovery time in the event that damage or attack occurs, and to identify the cause of damage or the source of attack for analysis by experts and/or investigation by law enforcement. It is therefore important that due to the specificity of each country, a policy is necessary to identify critical infrastructure and critical information infrastructure and protect these infrastructures as damage caused by a cyber-attack can severely jeopardize all national activities.

It is also imperative that governments within the region encourage the development of a self-sustaining Micro-Small and Medium Enterprises based cyber secured solution economic subsector driven principally by suitably empowered young knowledge workers that results in job creation, wealth generation, and subsequent government income through taxes.

The digital transformation of ECOWAS member countries that are developing rapidly will not be profitable for the region and its fellow citizens unless the region equips itself with instruments that provide credibility to make reliable and secure electronic communications and to protect critical information infrastructures. ECOWAS, therefore, needs to improve its involvement in the establishment of a trustworthy cyber space by providing better guidance and practical assistance to countries according to their needs. Such assistance includes cybersecurity strategy development, enacting and implementing appropriate legislation, promoting cybersecurity awareness and cooperation, creating a skilled cybersecurity workforce, and the establishment of necessary cybersecurity and cybercrime entities.

References

- Bada, M., Von Solms, B., & Agraftotis, I. (2018) *Reviewing National Cybersecurity Awareness in Africa: An Empirical Study*. Available from: www.thinkmind.org/index.php?view=article&articleid=cyber_2018_6_20_80051 [accessed 10 December 2018].
- Cole, K., Chetty, M., LaRosa, C., Rietta, F., Schmitt, D.K., & Goodman, S.E. (2008) *Cybersecurity in Africa: An Assessment*. Available from: www.researchgate.net/publication/267971678_Cybersecurity_in_Africa_An_Assessment [accessed 10 December 2018].
- ECOWAS (1979) *Protocol A/P.1/5/79 relating to Free Movement of Persons, Residence and Establishment*. Available from: http://documentation.ecowas.int/download/en/legal_documents/protocols/PROTOCOL%20RELATING%20TO%20%20FREE%20MOVEMENT%20OF%20PERSONS.pdf [accessed 10 December 2018].
- Global Cyber Expertise Magazine Issue 2 (2016) *Cybersecurity and the Fight Against Cybercrimes in West Africa: Current Status, Challenges and the Future*. Available from: www.thegfce.com/about/news/2016/12/07/cybersecurity-and-fight-against-cybercrimes [accessed 10 December 2018].

- GSM Association (2018) *The Mobile Economy West Africa 2018*. Available from: www.gsmainelligence.com/research/?file=e568fe9e710ec776d82c04e9f6760adb&download [accessed 10 December 2018].
- International Telecommunication Union (ITU) (2017) *Global Cybersecurity Index 2017*. Available from: www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf [accessed 10 December 2018].
- Jamil, Z. (2016) *Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime*. Global Action on Cybercrime Extended. Available from: <https://rm.coe.int/16806bf0f8> [accessed 10 December 2018].
- Roller, L.-H. & Waverman, L. (2001) *Telecommunications Infrastructure and Economic Development: A Simultaneous Approach* American Economic Review, 91(4): 909–923. Available from: https://www.jstor.org/stable/2677818?seq=1#page_scan_tab_contents [accessed 10 December 2018].
- Schia, N. (2018) The cyber frontier and digital pitfalls in the Global South. *Third World Quarterly*. Available from: <https://doi.org/10.1080/01436597.2017.1408403> [accessed 10 December 2018].
- Serianu (2016) *Africa Cyber Security Report – Achieving Cyber Security Resilience; Enhancing visibility and increasing Awareness*. Available from: www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf [accessed 10 December 2018].
- Serrano, A.S. (2015) Cybersecurity: Towards a global standard in the protection of critical information infrastructures. *European Journal of Law and Technology*. 6(3). Available from: <http://ejlt.org/article/viewFile/396/592> [accessed 10 December 2018].
- Whitty, M.T. (2018) 419 – *It's just a Game: Pathways to Cyber-Fraud Criminality emanating from West Africa*. Available from: <http://cybercrimejournal.com/WhittyVol12Issue1IJCC2018.pdf> [accessed 10 December 2018].

21

RISK, RESILIENCE, AND RETALIATION

American perspectives on international cybersecurity

James A. Lewis

The liberal institutions created after 1945 are being challenged by powerful new states, by understandable populist discontent in Western democracies, and by revanchist powers. This evolving political environment creates tension and conflict. Cyberspace is a principal domain for this conflict. At the same time, many researchers and officials in the US have concluded that no information technology can ever be made completely secure against advanced and persistent opponents (DOD, 2018, p. 3). This leads them to conclude that a defensive strategy will always be inadequate. The effect of this combination of increasing conflict and inadequate defense has been to reshape the America perspective on international cybersecurity.

Strategic context

Authoritarian regimes are challenging the US and the West, often in concert. The international balance of power has shifted away from the transatlantic centre, and countries want to push back against what they see as unwarranted interference in their internal affairs (once justified as democracy promotion) and a triumphalist United States. These challenges will usually not take conventional forms, since coercive international acts increasingly rely on cyber operations. Coercing and the threat to use force are displacing the rule of law.

One product of this larger global political restructuring is that the ‘Green Book’ era of Internet governance has ended. This has implications for international cybersecurity as nations redefine their objectives and expand their roles in cyberspace. The Green Book was the US policy document laying out how the Internet could be lightly governed and regulated by a new kind of transnational multi-stakeholder political system, where civil society and corporations would be equal partners to governments. This approach reflected the utopian beliefs of the 1990s regarding the future of international relations and the ‘end of history’ of international and ideological conflict (Fukuyama, 1992). Its most important assumption was the force and military power would be less important and that states no longer had a monopoly on the instrument of force. This belief was sadly mistaken – the ability of states to bring immense resources and to combine cyber with conventional military and intelligence assets gives them an unmatched advantage in the exercise of power – particularly if a state

is not constrained by the etiquette and rules of Western law. One unintended consequence of this is that cyberspace has become an untrammelled space for conflict and crime.

For a time, the Green Book was deemed adequate, but many states now reject millennial governance and are asserting sovereign control over national networks to provide for public safety and advance their national interests. The US is struggling to define a new approach. These interrelated trends of an increasing role for state in cyberspace and the indefensibility of networks define the larger political context in which American cybersecurity policy now operates.

There is interplay between the larger national security policies and cybersecurity. When the US in 2010 unwisely announced a 'redline', where on the Syrian use of chemical weapons against civilians was unacceptable and would meet with prompt retaliation, only to back down a few months later, other nations likely took it as a signal that perhaps they had overestimated the risk of actions against the US (DW, 2012). It is interesting that the cyber actions against Sony, GitHub, and the Sands Casino, dramatic escalations in coercive cyber operations against the US, occurred after the back down. After the Sony incident, the US began to work to repair the credibility of its international cyber policy by highlighting its improved attribution capabilities (explained in a single sentence in the 2015 State of the Union Address) and, since 2016, pursuing a policy of imposing consequences on cyber attackers (TICLJ, 2018).

Iran was responsible for the Sands attack. This did not receive similar public attention because, according to administration officials, there was a desire to avoid any risk of disrupting the nuclear talks with Iran, which some senior administration officials saw as the overriding, Peace Prize-worthy, foreign policy achievement (perhaps the only foreign policy achievement) of the Obama Administration. If nothing else, this highlights that cyber policy is not *sui generis* but must be analyzed in the larger context of security relations among states and a nation's foreign policy objectives. It is in this larger context of national strategies and objectives that US cyber policy has developed. It is possible, for example, the Trump Administration has been restrained in taking action against China for its cyber espionage both because espionage, unlike more coercive acts, falls into a legal grey area that the US itself inhabits and because it did not wish to complicate ongoing trade talks.

One result of the realization that no network can be guaranteed to resist persistent efforts by an advanced attacker is an increased emphasis on risk-management (rather than the eradication of risk) and on resilience in cybersecurity planning. The emphasis on risk management and resilience assumes that opponents will be able to gain access to networks and the goal should be to ensure continued provision of critical services in a degraded network environment. Much of the reorganization of cybersecurity functions at the Department of Homeland Security is driven by this conclusion. However, the conclusion that no technical defense will be adequate also has serious implication for the US approach to international cybersecurity and has led to a fundamental reorientation.

Negotiation

The most significant implication is a change from an emphasis on developing norms of responsible state behavior to one on implementing norms (those agreed to in the United Nations) and imposing consequences on malicious cyber actors who violate or transgress accepted norms. Response and retaliation will help set the boundaries of permissible action in cyberspace. Nations need to respond to hostile cyber actions if they are to establish the boundaries of permissible behavior. No other method is likely to be effective.

There is, of course, an interplay between the development of norms and responsive actions. Both are needed for controlling cyber activities. But the norms and confidence building measures (CBM) approach assumed shared values among nations and a common interest in stability. It is fair to say that US policymakers no longer believe this to be the case. The change is the product of a more conflictual international environment, increasing action by hostile states against US sovereignty and interests in cyberspace, and a sense that additional norms are unnecessary, all reinforced by the skepticism with which the current administration regards arms control.

To be fair, there is some justification for this skepticism. All parties are moving away from the strategic arms agreements from the 1980s and earlier; they were not written for the current security environment, if only because there are now three strategic players and not two. A strategy based on creating norms for responsible state behavior, reinforced by confidence building measures that increased transparency, predictability and the scope for cooperation, initially met with some success, embodied in three agreed reports in 2010, 2013, and 2015 from the UN Group of Government Experts (GGE), composed of the five members of the UN Security Council and 20 other nations (UNGA, 2010; 2013; 2015). The GGE reports laid out recommendations for cybersecurity norms, CBMS and capacity building measures, culminating in endorse of the recommendation by the UN General Assembly, which called on member states to be guided by the conclusion of the 2015 Report of the Group of Government experts. However, the last GGE in 2017 failed to reach agreement (e.g. Tikk & Kerttunen, 2018).

While the scope for international agreement is constrained by the conflictual international environment and the end of Green Book millennialism, there are opportunities. International agreement could usefully develop constraints on the use of cyber-attacks by banning some categories of attacks entirely. This is the area where the interests of opposing states are most likely to overlap. US policy is to work with likeminded nations to operationalize norms and consequences, while continuing to explore whether further agreement with opponents is possible at the margins of what was agreed in the UN General Assembly in 2015.

A new and complicated round of cyber negotiation will begin later in 2019, meaning there is room for progress on international agreement, but in the near term, and given the preference of this administration, the US has adopted a different approach. The current administration believes that the goals of its cyber opponents for an agreement on cybersecurity are largely intended to impede the US and its allies more than themselves (given the difficulties of verification and the belief that that few would abide by such agreements) is innately attractive to the more nationalist and suspicious administration. (The White House, 2018)

Agreements among like-minded states developing parallel negotiating processes to a “global” approach involving opponents could endorse and reinforce existing commitments to human rights in their extension into cyberspace and the multi-stakeholder model of Internet governance, perhaps developing ideas on how to Western-centric multilateralism to accommodate non-Western states.

It is worth remembering, however, that the development of agreement on nuclear and other weapons of mass destruction only began after the Cuban Missile crisis, when the two leading nuclear powers were confronted with a potentially existential conflict. We may need to wait for some similar existential for progress in cybersecurity negotiations. Cyber-attack does not pose an existential threat, at least yet, and is no way comparable to the risk of strategic nuclear war. This reduces the incentives of agreement among all powers, including the US. In any case, the fluid state of international politics (with some nations rising and other falling) makes achieving an effective and lasting agreement more difficult.

The imposition of consequences

The United States cybersecurity policy has changed significantly under the Trump administration. The key change is a decision by the US that its cyber opponents are unlikely to change their behavior without the imposition of consequences (a similar conclusion on the necessity of response was reached by the European Union). (The White House, 2018; Moret & Pawlak, 2017) A number of factors contributed to this decision, including a general unhappiness with the perceived indecision and timidity of the previous administration, the development of operational capabilities at cyber command, and recognition that the most damaging cyber incidents were perpetrated by State actors.

The Trump Administration's *National Security Strategy* (issued in its first year in office), promised a 'clear-eyed' view of the world and challenges the US faces. The strategy paints a more conflictual multipolar environment and emphasizes 'great power' competition with China. The theme of cybersecurity and cyber as a new domain for conflict is woven throughout the text ('cyber' appears 45 times in the text, the same number of times as 'nuclear'). This perception of a world marked by inter-state rivalry and coercion 'below the level of conventional military conflict,' where the principle domain for engagement is cyberspace, informs the US approaches to cybersecurity (The White House, 2017).

Current US cyber policy stands marked in contrast to that of its predecessor, which can be described as legalistic and timid (it knew, for example of election interference in April 2016, had developed a response plan involving both overt and covert action by August, but was unable to decide whether to act until the very end of its term in 2016). The Obama administration's legalism impeded effective US responses to hostile cyber actions, and involved debates over whether an US retaliatory act would violate the sovereignty of the nations whose networks it traveled (similar to the overflight issues that appears in military air actions), and whether it was necessary to first ask the permission of those nations before acting. This indecision has been greatly reduced in the Trump administration.

The increased tempo of indictments against malicious cyber actors by the Department of Justice is one indicator of this more assertive approach to cybersecurity, but there is a general recognition that indictments, while useful and important, are not enough. Indictments are on the lower end of possible responses allowed under international law. What more should be done is an area of divergence and perhaps even competition in US policy.

The two avenues for imposing consequences being pursued by the US are 'persistent engagement' and what could be called 'collective deterrence.' The first has a unilateral focus (although joint actions with close allies can be part of this) (USCYBERCOM, 2018). The second involves developing a common approach among likeminded nations to respond when there are malicious actions that clearly depart from the norms of responsible state behavior develop in the UN (particularly the 2015 Report of the UN Group of Government Experts, which the General Assembly called on all member states to observe (DOS, 2018).

The new policies (and their implementations) do not come without risk, chiefly of escalation, and one of the tasks for the US is to develop the policies and practices that would accompany any action to reduce this risk. Do you tell an opponent in advance? Do you leak the action afterwards (as occurred with the Washington Post story on cyber command blocking Russia's Internet Research Agency around the time of the 2018 midterm elections)? (WP, 2018). Does the US inform allies or request their support? Even unilateral military actions by the US will need to be embedded in some sort of diplomatic strategy that has yet to be announced.

The supporters of persistent engagement are vehement in their desire not to use the term 'deterrence': for example, the US Cyber Command 2018 Vision elaborating the doctrine of

persistent engagement mentions deterrence only once (USCYBERCOM, 2018). This is at least partially a reasonable objection. Old style nuclear deterrence was predicated on the idea that the weapons would never be used. This is definitely not the case in cyber operations, where the US and its cyber opponents are in weekly (if not daily) contact, according to US military sources, and cyber operations are the norm. In general, the discussion of cybersecurity in the US (at least in academic circles) is hampered by an overreliance on nuclear era concepts that are inappropriate for a new kind of international politics and a very different kind of 'weapon'. Concepts like deterrence or strategic stability may hamper analysis more than aid it, since our leading opponents do not think in these terms (and some scholars, such as Keith Payne, suggest that that the Soviets, even at the height of the nuclear strategy, did not understand what the US was saying about signaling, compellence, or the granularity of deterrence strategy (e.g. Schelling, 1966; Payne, 2001).

The chief drawback to persistent engagement is the risk of repeating larger US failings in developing coherent international strategies. The central assumption that underlay US strategy since 1990 on the inevitable triumph of Western democracy is no longer tenable. The US has had persistent engagement in Afghanistan for fifteen years, but in the absence of a coherent strategy, this engagement has been fruitless. Since the US is not going to defeat and remake its opponent in the grand style of 1945, it will need to reach some accommodation that reduces the risk of warfare and in cyberspace, involves changing their calculation of the risks of cyber actions against the US. Persistent engagement only makes sense if it is linked to seem larger strategy, and the US has not had a real strategy in three decades. Old style deterrence does not make sense as unlike nuclear forces, these are 'weapons and forces that will be used, but that is not the same as saying that a persistent campaign of deliberate engagement to change opponent risk calculation is unnecessary. The assumption that underlies persistent engagement is that a few sharp rebukes, described in US policy as 'temporary, painful, but reversible', will reset opponent analysis of the benefits of continued cyber action against the US.

This comes with the risk of escalation of conflict, in cyberspace and elsewhere, but this risk can be managed through diplomatic action (including public diplomacy) and by accurately calculating a blend of proportionality and an opponent's appetite for risk, e.g. responses that are both sufficient and unlikely to provoke an escalatory response – both being areas that require further work and experience. In any case, there is an assumption that we are entering a conflictual environment against implacable hostile opponents where the risk of increased conflict is unavoidable. In terms of American bureaucratic politics, this best describes the view of the defense and military establishment against which an enfeebled diplomatic bureaucracy lacks both influence and coherent alternative policies.

Wrangling over evidentiary standards misses the point. International relations do not follow the logic of the courts and legal reasoning; they follow the logic of power and relations between sovereigns. There has been an effort in the last century to create legal structure to guide state action, but this remains secondary and should not obscure the centrality of power. The rules for great power politics are not the same as a court, if a country wants to remain a great power. This is politics, not jurisprudence and there are the audiences for any action are the attacker and the international community, all of whom are watching what the US will do. Holding to a legal evidentiary standard only increases the likelihood of indecision and continued opponent action against the US.

The collective deterrence approach also faces policy challenges. The most important of these are the need for collectively acceptable answers to the questions of attribution and proportionality of any response. As one Washington's European ally put it, to join the US

in some kind of retaliatory action, they would need the support of their ministers and their public, and this support can only be gained by the provision of credible information. The US damaged its credibility of its intelligence during the Iraq war, but the greater obstacle is that attribution can at times rely on sensitive sources or methods that the US could be reluctant to disclose.

Similarly (and this slows the development of persistent engagement), there is not enough experience to easily determine proportionality of a response to a malicious cyber action. Most cyber operations occur in a grey area that falls below the threshold of the use of force. This complicates the development of an appropriate response by reducing the applicability of precedent. These problems will be difficult to resolve without more experience in cyber operations (which in itself, engenders risk), but theoretical or academic decisions may have only limited utility.

The most immediate response is likely to be to use legal tools for retorsion and counter-measures. The non-forceful options for response include information operations – such as damaging counter leaks about corruption or governmental indifference to citizen welfare – indictments, sanctions, or some other public censure. Covert actions could include tampering with or erasure of financial accounts. Military actions that produce coercive effect or cross the use-of-force threshold are riskier, given the confrontational attitude found in many authoritarian regimes, but the US is attracted to limited military cyber operations, accompanied by an effective diplomatic strategy, and may be necessary to change the risk calculation of opponents. Other options might include some kind of stricture on an attacker's Internet connectivity, but the ability to carry out this kind of action is not well developed.

Since the evidentiary standards for imposing sanctions are lower than for indictments (in the US), they might be preferred. Sanctions are also a more flexible tool than indictments, more visible than covert action, and they displease all opponent regimes (this is not “name and shame” – always an academic conceit, as one does not shame a great power, but the irritation created by restrictions on travel and finance) (Finnemore & Hollis, 2019). All this makes legal and financial actions attractive options, but after numerous sanctions, the behavior of America's four primary opponents has not changed. Sanctions are a good first step, but additional measures are necessary. The US and its allies need to consider whether to use cyber operation against opponents, perhaps similar to what Joint Task Force Ares was able to do against ISIS (the details of JTF Ares actions remain classified by the US and participating allies), but any military action would need to be carefully considered and managed to ensure proportionality and to manage the risk of escalation. In the language of arms control, the US and its allies need to populate all the rungs of the deterrence ladder with appropriate and proportional responses to hostile cyber actions.

Strategy for uncertainty and conflict

In the absence of agreement, and in light of the increasing tempo of hostile cyber actions, the US has decided that it must respond to hostile cyber actions if we are to establish the boundaries of permissible behavior in cyberspace. This leads to the more difficult question of defining an appropriate response, as the ‘weaponization’ of speech, delivered by social media enabled by the Internet, is not a problem envisioned in the existing rules of armed conflict. The goal for policy should be to change this, building the precedents for attribution, response, and thresholds established by US actions against other cyber opponents. Hacking should not be penalty free if we want it to stop.

The emphasis on persistent engagement and collective deterrence and the likely hindrances to a negotiated agreement to end or reduce cyber-attack means that the US is entering a new era of international cybersecurity policy, one that is more conflictive and that comes with greater risk of warfare. The alternative – continued victimization – is unappealing, but the US has only begun to develop the policies, strategies, and instructional instruments needed to guide it in a more dangerous and fluid cyber environment. US policy is slowly coming to recognize the world as it is, conflictive and dominated by states, and not as we imagined it when the United States was unchallenged. The powerful economic and political forces that are reshaping international relations mean, however, that conflict is more likely than peace, and US policy has begun adjusting to recognize this.

References

- Department of Defense (DoD) (2018) *Summary. Department of Defense Cyber Strategy*. Available from: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.PDF [accessed 3 June 2019].
- Department of State (DoS) (2018) 'Recommendations to the President on deterring adversaries and better protecting the American people from cyber threats'. Office of the Coordinator for Cyber Issues (May 31). Available from: www.state.gov/recommendations-to-the-president-on-detering-adversaries-and-better-protecting-the-american-people-from-cyber-threats/ [accessed 3 June 2019].
- Deutsche Welle (DW) 2012 'Obama's policy failed to contain Syrian crisis'. Available from: www.dw.com/en/obamas-policy-failed-to-contain-syrian-crisis/a-19488044 [accessed 6 June 2019].
- Finnemore, M. & Hollis, D.B. (2019) 'Beyond naming and shaming: Accusations and international law in cybersecurity'. *Temple University Legal Studies Research Paper No. 2019-14*.
- Fukuyama, F. (1992) *The End of History and the Last Man*. New York: Free Press.
- Joint Chiefs of Staff (2018) *Cyberspace Operations* (JP 3–12). Available from: www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150 [accessed 3 June 2019].
- Moret, E. & Pawlak, P. (2017) 'The EU cyber diplomacy toolbox: Towards a cyber sanctions regime?' Available from: www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf [accessed 3 June 2019].
- Payne, K. (2001) *The Fallacies of Cold War Deterrence and a New Direction*. Lexington: University Press of Kentucky.
- Schelling, T. (1966) *Arms and Influence*. New Haven, Yale University Press.
- Temple International and Comparative Law Journal (TICLJ)* (2018) 32(2).
- The White House (2017) *National Security Strategy of the United States of America*. Available from: www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf [accessed 3 June 2019].
- The White House (2018) *National Cyber Strategy of the United States of America*. Available from: www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [accessed 3 June 2019].
- Tikk, E. & Kerttunen, M. (2018) *Parabasis. Cyber-Diplomacy in Stalemate*. Norwegian Institute of Foreign Affairs. 5/2018.
- United Nations General Assembly (UNGA) (2010) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/65/201 (30 July).
- United Nations General Assembly (UNGA) (2013) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (24 June).
- United Nations General Assembly (UNGA) (2014) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (22 July).
- United Nations General Assembly (UNGA) (1998) Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, A-C.1–53–3, (30 September).

- United States Cyber Command (USCYBERCOM) (2018) *Achieve and Maintain Cyberspace Superiority Command Vision for US Cyber Command*. Available from: www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010 [accessed 3 June 2019].
- United States Department of Defense (DOD) *Summary of the National Defense Strategy Sharpening the American Military's Competitive Edge*. Available from: <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf> [accessed 3 June 2019].
- Washington Post* (WP) (2019) 'U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms' (February 27). Available from: www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html?utm_term=.a2218d05fa69 [accessed 3 June 2019].

INTERNATIONAL INFORMATION SECURITY

Problems and ways of solving them

*Andrei V. Krutskikh and Anatoli
A. Streltsov (translated by Eneken Tikk)*

The discussion of the problems of international information security (IIS) at the 73rd session of the UN General Assembly showed that the international community still cannot determine its priorities in countering the existing and potential threats of malicious and hostile use of information and communication technologies (ICT). For the first time in the history of the United Nations, member states adopted two resolutions on the same issue during one session at the initiative of the Russian Federation and the United States (UNGA, 2018a; UN ODA, 2019). Both resolutions provide for the continuation of the study of existing and potential threats in the field of information security and possible joint measures to address them, as well as the problems of applying international law to the use of ICT by states.

To accomplish this task, the Resolution (73/266) adopted at the initiative of the United States proposes the creation of a group of government experts on achievements in the field of informatization and communications in the context of international security, while the Resolution (73/27) adopted on the initiative of the Russian Federation provides for the creation of an Open-Ended Working Group oriented as priority for the further development of norms, rules and principles of responsible behaviour of states in the field of ICT, the study of the possibility of organizing regular dialogue under the auspices of the UN. As can be seen from the mandates of these groups, there is some overlap in the objects of their study.

This chapter sets out the opinion of Russian experts on the reasons for the adoption by the UN General Assembly of two resolutions on IIS. It also formulates some proposals on the priority areas of work of the Open-Ended Working Group.

The current international information security affairs and their causes

Among the causes of the situation must be considered, first of all, the novelty of the ICT environment as a space for international cooperation of states in the field of international peace and security, as well as a significant gap between the states of the world in the use of ICTs to ensure the sustainable development of society, often called ‘the digital divide’.

The novelty of the ICT environment as a space for international cooperation rests on the fact that the need for interaction between states on ensuring the security of the use of ICT, information and communication networks has arisen relatively recently (UNGA, 1998, pp. 2–3). For a long time, the expert community sincerely assumed that the development of

the Internet can be organized primarily on the basis of self-governance, and that the participation of states in this activity should be quite limited (WSIS, 2005). It later turned out that the warning of the Russian Federation about the possibility of threatening international peace and security through the malicious and hostile use of ICT on the Internet was well grounded.

After ten years (2003–2013) of studying the problem, government experts included the following provisions in the Report of the Group of Governmental Experts on Developments in Information and Communications in the Context of International Security in 2015 by consensus:

States bear the primary responsibility for ensuring state security and the safety of their citizens, including in the ICT environment

[...]

International law, and in particular the Charter of the United Nations, is applicable and essential to maintain peace and stability and to promoting an open, secure, stable, accessible and peaceful ICT environment.

(UNGA, 2015, #19 and #24).

Studying the problems of organizing practical international cooperation on the basis of these provisions revealed significant differences between the ICT environment and other spaces of international cooperation – land, sea, airspace and subsoil (Streltsov, 2017).

First, the ICT environment, the basic infrastructure of communication networks and the global Internet, is man-made. The ability of the ICT environment to promote international cooperation in the use of ICTs for the transmission and processing of information substantially depends on commercial organizations operating in various jurisdictions. These organizations are the owners and administrators of technical devices of communication networks and the Internet, providing communication services, processing and disseminating information, enabling remote access to the required data.

Processing and transmission of information on the Internet is carried out using a global system of digital identifiers (such as domain names, and digital addresses). The operation of the addressing and navigation system is supported by the non-profit organization International Address and Domain Name Corporation (ICANN).

Given the fact that the United States has not assumed any international obligations to ensure the sustainability of the Internet, and ICANN is not a subject of international law, therefore lacking international legal capacity, transaction capacity and responsibility, the stability of functioning and the safety of using devices and systems in the ICT environment is dependent on the political situation in individual states.

Second, the use of ICTs for automated processing and transmission of information is virtual, making it difficult to observe. This complicates providing evidenced confirmation to an incident in the ICT environment and identifying the states involved in its occurrence, as well as involving independent experts in assessments of the negative consequences of the incident. At the same time, the participation of witnesses and independent experts is one of the conditions for the possibility of resolving international disputes by peaceful means, as recommended by the UN Charter – ‘by negotiations, consultation, mediation, conciliation, arbitration, trial’, and other means. (UN, 1945, Art. 33).

It is significant that since the emergence of international disputes over incidents in the ICT environment, these means have never been used.

Third, in the ICT environment there are no internationally recognized borders to zones of states’ responsibility, i.e. the spatial limits of their sovereignty remain uncertain. The

solution to this problem by 'linking' the national segments of the ICT environment to the territory (ref. 'the jurisdiction of states over the ICT infrastructure within their territory' (UNGA, 2015, #27) requires concretization, providing legally reliable information about incidents in the ICT environment and about the states involved in these incidents.

Thus, on the one hand, only international cooperation of states can ensure the existence of a global ICT environment as a factor in the development of society, and on the other, existing principles and norms of international law are not able to have an ordering effect on the cooperation of states in creating an open, safe, stable, accessible, and peaceful information environment. The above allows us to conclude that there is a certain 'crisis' of international law. As a result of this 'crisis,' the main arguments in disputes over incidents in the ICT environment, as well as the main means of preventing malicious and hostile use of ICT by states, are increasingly threats of the use of force.

Some states are promoting the concept of the legitimacy of using malicious ICTs as a means of exercising the right to individual and collective self-defence. The same states are actively promoting the idea of preventing the threat of malicious or aggressive use of ICTs by emphasising deterrence by punishment and collective responses (Stoltenberg, 2019), even inflicting the so-called 'preventive cyber-attacks', and conducting other violent actions against the independent states without the appropriate decision of the UN Security Council

Attempts are being made to fill the gaps in the legal regulation of international cooperation in the ICT environment by promoting the concept of 'collective attribution' and collective counter-measures' (Kaljulaid, 2019), based on the principle of 'naming and shaming'.

In the framework of this concept, a group of states that declares itself to have suffered from malicious or hostile use of ICTs considers it legitimate, without showing evidence, to attribute international legal responsibility to states that are allegedly responsible for the occurrence of the incident. This suggests that evidence of the involvement of 'guilty' states in such incidents can be replaced with the conviction of the international community that the attribution of responsibility is just. The 'campaigns' in the Western media testify of attempting to turn groundless accusations against the Russian Federation of interfering in the elections in the USA (2016), violating of the terms of the Treaty on the Elimination of Intermediate-Range and Shorter-Range Missiles (2018) and other events, into international legal practice. Such actions can result only in increased danger of conflicts that threaten international peace and security.

It can be assumed that the 'crisis of international law' in relation to the ICT environment is quite comfortable for some states, above all, the USA, which, as President of the Russian Federation Vladimir Putin noted, is used to replacing 'general international rules with laws, administrative and judicial mechanisms of one country or group of influential states, seeking to extend its jurisdiction to the whole world' (Putin, 2019). It is hardly possible to explain in another way the refusal of the United States and its allies to support the proposal of the Russian Federation and some other states to endorse by the 73rd session of the UN General Assembly, consensus formulations of norms, rules and principles of responsible behaviour of states in the ICT environment.

An important factor that led to the adoption by the 73rd session of the UN General Assembly of two resolutions is also the digital divide between developed and developing states. This gap lies in the significant difference between the levels of ICT use achieved by these states to solve the problems of economic development, public administration, and ensuring human rights and freedoms in the field of information activity.

At the World Summit on the Information Society, it was noted that 'bridging the digital divide and ensuring a harmonious, fair and equitable development for all will require the

firm determination of all stakeholders’, ‘digital solidarity both at national and international levels’ (WSIS, 2003, #17). The digital divide is manifested in the fact that, as noted in the Report of the Group of Governmental Experts in 2015, ‘some States may lack sufficient capacity to protect their ICT networks. A lack of capacity can make the citizens and critical infrastructure of a State vulnerable or make it an unwitting haven for malicious actors.’ (UNGA, 2015, #19). The lack of sufficient capacity in the field of ensuring international information security is a serious obstacle to identifying and assessing the main threats to the information security of the national infrastructure, as well as ways to counter these threats, including through international cooperation. These unresolved issues have a significant negative impact on the effectiveness of international cooperation in creating an open, secure and peaceful ICT environment.

The need for legal clarity and certainty

In the current circumstances, it seems important to intensify efforts aimed at creating legal guarantees of objectivity and impartiality in assessing incidents in the ICT environment, in attributing states involved in an international dispute over such incidents, as well as implementing measures to smooth out differences in state capacities in the field of counteraction to potential and existing threats of IIS.

The progressive development of international law in the field under consideration would be advisable to focus on the following tasks:

- delimitation of areas of responsibility of states for the safe use of ICTs by subjects of public life under their jurisdiction;
- clarification of international obligations of states in the field of the ICT environment arising from the UN Charter, other general and special international conventions, international custom, general principles of law recognized by civilized nations, and other sources of international law;
- the creation of mechanisms for international cooperation in the collection of legally reliable information about incidents in the ICT environment, as well as the development of an appropriate system of technical regulation standards providing the possibility of obtaining such information;
- the formation of an organizational and legal mechanism for resolving international disputes over incidents in the ICT environment.

The delineation of the areas of responsibility of states in the ICT environment creates the conditions for translating into practice the recommendations on the applicability of ‘sovereignty and 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’ (UNGA, 2018b).

When performing this task, it is necessary to take into account that the implementation of information processing and transmission technologies is carried out in the space of global digital identifiers, which are not legally attached to the traditional territory of states. The current system of maintaining digital identifiers is based on international private law, as identifiers are owned by individuals who have received appropriate permission from ICANN. In this regard, international cooperation in the field of preventing the use of ICT infrastructure in the state to damage the ICT infrastructure of other states is possible only on the basis of international treaties that set procedures for delimitation and demarcation of

the borders of responsibility of states in the ICT environment, and principles for establishing a legal regime of these boundaries, ensuring compliance with international obligations of states in the ICT environment.

Clarification of international obligations of states in the ICT environment creates the conditions for the formation of a common understanding of their content in relation to ensuring the functioning and use of the ICT environment for the transfer, storage, processing and dissemination of information.

The implementation of this task involves the study of the problems of the progressive development of international law in relation to the cooperation of states in the ICT environment, regulated by: the principles of international law enshrined in the United Nations General Assembly Declaration of Principles of International Law Concerning Friendly Relations and Cooperation (UNGA, 1970), the norms of international treaties on the maintenance of international peace and security, as well as the norms of international humanitarian law.

The fulfilment of this task would allow us to find answers to many outstanding issues of international cooperation, including (Krutskikh & Streltsov, 2014):

- countering the threats of malicious and aggressive use of ICT by states (UNGA, 1974);
- stipulation of uses of malicious ICTs, which can be considered as an armed attack, creating conditions for the application of the inalienable right of states to individual and collective self-defence, as well as actions prohibited by international law for humanitarian purposes;
- exchange between states of information about incidents in the ICT environment, including that used to resolve relevant international disputes by peaceful means;
- providing critical international legal protection to critical facilities of the national information infrastructure, as well as other civilian facilities of the information infrastructure;
- attribution to states of international legal responsibility for incidents in the ICT environment;
- determination of the boundaries of armed conflict in the ICT environment, as well as the legal status of neutral states;
- countering the use of ICTs to interfere in the internal affairs of sovereign states;
- sustainability of Internet governance;
- participation of international organizations in the settlement of international disputes over incidents in the ICT environment, including those arising from the inclusion of hidden malicious functions in software products sold on the market.

Given that the progressive development of international law in these areas is carried out in an environment where the international community does not yet have experience in solving such problems, it is important to minimize the risks of conflicts due to misunderstandings. For this reason, the Russian Federation considers it important to begin to clarify the international obligations of states by developing the principles of international law. The first step towards clarifying the obligations arising from the principles of international law are the recommendations regarding the norms, rules and principles of responsible behaviour of states in the ICT environment. The adoption of these norms, rules and principles will create the basis for working out the interaction of states in using peaceful means of resolving international disputes over incidents in the ICT environment (for an analysis of the 2015 GGE recommendations for norms, see Tikk, 2017).

The next step could be to clarify international obligations in the ICT environment arising from treaties and other sources of international security law, as well as international

humanitarian law. The difficulty in reaching agreement on these issues is largely explained by the possibility of dangerous consequences for the national security of states, and the international community, in the event that states have different interpretations of these obligations in relation to actual incidents in the ICT environment, as well as discrepancies in the views of states on the 'perpetrators' of incidents and assessment their consequences. For this reason, clarification of international obligations would have to be carried out in the process of a comprehensive discussion between the UN member states.

An important area of international cooperation of states in the ICT environment in order to maintain international peace and security is the development of a system of technical regulation standards that provide the possibility of obtaining legally reliable information about incidents in the ICT environment. The relevance of this field of cooperation results from the artificial, technical nature of the ICT environment and the virtual nature of the processes for implementing information processing and transmission technologies. Reaching agreements in this area will create the material basis for creating an international system for monitoring the implementation by states of their international obligations in the ICT environment.

This task has significant impact on the development of the processes of applying peaceful means of resolving incidents and, as a result, the need for the participation of experts in the field of technical, political and legal issues of the use of ICT in the development of technical regulation standards and mechanisms for compliance with these standards by all entities ensuring the functioning of ICT environment.

Finally, the global nature of the ICT environment makes it important for the formation of an international information security system to fulfil the task of reducing the differences in states' capacity in the field of countering potential and existing IIS threats. Studying of ways to solve the problem of capacity building of states is included in the mandate of the Open-Ended Working Group and the Group of Government Experts created on the basis of relevant resolutions of the 73rd session of the UN General Assembly (RES 73/27 and RES 73/266, respectively). This dual process creates the basis for developing common approaches to solving the problem.

Leads for the work of the Open-Ended Working Group

The main priorities of the Open-Ended Working Group could be as follows:

First, adoption of norms, rules, and principles of responsible behaviour of states in the ICT environment. In 2018, the 73rd session of the UN General Assembly by an overwhelming majority of votes for the first time approved the initial list of such norms, rules and principles. This is a unique achievement for the international community. The adoption of the list creates the basis for the implementation of necessary measures to create an open, safe, stable, accessible and peaceful information environment, preventing conflicts caused by incidents in the ICT environment, and consolidating the interpretation of the principles of international law, such as the principle of the non-use of force, as applied to the ICT environment, respect for sovereign equality, the principle of non-interference in the internal affairs of sovereign states, the principle of respect for human rights and freedoms, as well as the creation of conditions for ensuring security and the use of ICT environments. The mandate of the Working Group directs its work to preparing the international community to universally adopt these norms, rules and principles, and to find ways to ensure their practical application.

Second, the implementation of confidence-building measures in the ICT environment.

Based on the experience of regional cooperation, in particular international cooperation at the OSCE and the ASEAN Regional Security Forum, the Working Group could explore ways to create a universal list of such measures. It would be advisable to study the possibility of unifying confidence-building measures agreed in different regions, and to prepare proposals for the adoption of universal criteria for their further development.

Third, the study of the establishment of a permanent operating structure under the auspices of the UN authorized to discuss the problems of international information security with the participation of all interested states. The creation of such a structure would allow all interested states to be included in the discussion of the problem, as well as contribute to the fulfilment of the task of building the capacities of states that do not have sufficient capabilities in this area. The possibility provided by the resolution of the UN General Assembly to bring in the discussion of the problems of the necessary specialists, including experts of the International Telecommunication Union in the field of technical regulation, allows to give the discussion the necessary comprehensive character.

Fourth, assistance in building up the digital potential of developing states, studying measures to narrow the digital divide.

Fifth, the study of the feasibility of creating a legal mechanism for the use of peaceful means of resolving international disputes related to incidents in the ICT environment and the dissemination of 'fake' messages, including the creation of a special body to resolve disputes based on the consent of interested parties (arbitration body).

The successful work of the Working Group could enable the UN General Assembly to come to universal decisions that could ensure the beginning of a continuous negotiation process on IIS issues, as well as to some extent contribute to the success of the Group of Government Experts, created on the initiative of the United States and its allies. The conflict-free interaction between the two Groups will contribute to the integration of the international community in order to use ICTs, primarily for peaceful purposes for the benefit of all mankind and the sustainable development of all states.

The role of other stakeholders

To implement the identified priorities of the work of the Open-Ended Working Group, it seems important to actively support the expert community, interested commercial organizations and civil society organizations. In order to facilitate the participation of stakeholders and organizations in this activity, the National Association of International Information Security (NAIIS) has been created in the Russian Federation. The National Association is a voluntary participation corporate association of legal entities and individuals, created to facilitate the activities of its members in implementing the state policy of the Russian Federation in the field of IIS. Its founding institutions include Lomonosov Moscow State University, Moscow Institute of International Relations of the Ministry of Foreign Affairs of Russia, Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Diplomatic Academy of the Russian Ministry of Foreign Affairs, Norilsk Nickel, and *International Life* magazine.

The main objectives of the National Association are: assistance to public authorities in their activities to implement public policy in the field of IIS; assistance in objective informing and explaining to civil society organizations of the Russian Federation and foreign states the main provisions of the state policy of the Russian Federation in the field of IIS; and

assistance in the formation of a system for ensuring the sustainable functioning of global and national information infrastructures.

The Association brings together leading experts in the field of political, legal, technical issues of providing IIS, as well as leaders of Russian business, the success of which depends on the stability and security of the use of the ICT environment. An important aspect of the work of the National Association is cooperation with interested foreign expert organizations. The main venues of the National Association, which discusses IIB problems with foreign experts, are the annual International Forum 'Partnership of the state, business and civil society in ensuring international information security', held in April in Garmisch-Partenkirchen, and the Conference of the International Information Security Research Consortium, held in December in Moscow.

In the view of the National Association, its cooperation with foreign expert organizations could contribute to the successful work of the Open-Ended Working Group and the Group of Government Experts established by decision of the UN General Assembly by promoting a common understanding of the practical application of the norms, principles and rules of responsible behaviour of states in the ICT environment and ways to solve them, as well as determining ways to effectively use the potential of the expert and scientific community to increase security of commercial organizations in the ICT environment. Thus, even with the uncertain position of many states on the priority areas for the formation of the IIS system, the international community has means for jointly developing of an effective IIS system.

References

- Kaljulaid, K. (2019) President of the Republic at the opening of CyCon 2019. Speech at the NATO CCDCOE conference 'Silent Battle' Tallinn (29 May). Available from: <https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/> [accessed 11 July 2019].
- Krutsikh, A.V. and Streltsov, A.A. (2014) International law and the problem of international information security. *International Affairs*. 11.
- Putin, V.V. (2019) Speech at the St. Petersburg International Economic Forum (7 June). Available from: <http://en.kremlin.ru/events/president/news/60707> [accessed 9 September 2019].
- Stoltenberg, J. (2019) NATO will defend itself. *Prospect* (27 August). Available from www.prospectmagazine.co.uk/world/nato-will-defend-itself [accessed 9 September 2019].
- Streltsov, A.A. (2017) Adaptation of international law to the information space. Presentation at the International Information Security Research Consortium (IISRC) Forum 'Partnership of the State, Business and Civil Society at Ensuring International Information Security' (27 April).
- Tikk, E. (ed.) (2017) *Voluntary Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology. A Commentary*. Civil Society and Disarmament. UN Office for Disarmament. New York.
- United Nations (UN) (1945) *The Charter of the United Nations*.
- United Nations General Assembly (UNGA) (1970). *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*. Resolution 2625 (24 October).
- United Nations General Assembly (UNGA) (1974) *Defining Aggression*. Resolution 3314 (14 December)
- United Nations General Assembly (UNGA) (1998) Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Secretary-General, A/C.1/53/3 (30 September).
- United Nations General Assembly (UNGA) (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174 (22 July).
- United Nations General Assembly (UNGA) (2018a) *Developments in the Field of Information and Telecommunications in the Context of International Security*. Report of the First Committee. A/73/505 (19 November).

- United Nations General Assembly (UNGA) (2018b) *Developments in the Field of Information and Telecommunications in the Context of international Security*, A/RES/73/27 (11 December).
- United Nations General Assembly (UNGA) (2019) *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/RES/73/266 (2 January).
- United Nations Office for Disarmament Affairs (UN ODA) (2019) Developments in the field of information and telecommunications in the context of international security. Available from: www.un.org/disarmament/ict-security/ [accessed 9 September 2019].
- World Summit on Information Society (WSIS) (2003) Declaration of Principles Building the Information Society: A Global Challenge in the New Millennium. Geneva. (12 December).
- World Summit on Information Society (WSIS) (2005) Tunisian program for the information society. Second phase. (18 November).

PEOPLE'S REPUBLIC OF CHINA

Seven cybersecurity considerations

Zhang Li

To accurately understand and grasp China's cybersecurity strategy, it must be looked at from several angles. This chapter elaborates on various aspects – from the importance the Chinese government and leaders attach to cybersecurity to recognized new changes and new features of the current cybersecurity situation, to predictions of China's cybersecurity policy direction, and industrial and international considerations.

The Chinese government attaches great importance to network security

In recent years, President Xi Jinping has repeatedly given instructions on cybersecurity and made requests concerning it. In 2018 alone, President Xi Jinping put forward four requirements at the National Conference on Cyber Security and Informatization:

First, he said, it is necessary to establish a correct view of network security. That is to realize that 'there is no national security without cybersecurity', recognizing that key information infrastructure has become the nerve centre of key industries related to national economy and people's livelihood such as finance and transportation. Protecting the key information infrastructure is the top priority of the Chinese government's network security work.

Second, establishing the cyber and network security of the people depends on developing people's thinking. The focus is on improving the awareness of cybersecurity among the whole community and improving the security protection skills of the whole society.

The third requirement is to pay attention to core technologies. Although the current international system has, for decades, been based on the international division of labour and global trade, Western countries led by the United States have been imposing restrictions on China in key technology areas (the Wassenaar Agreement is an example of such a regime). China is reluctant to be controlled by other countries in the core field of technology.

Fourth, China's adherence to cyberspace governance should include multilateral participation and multi-participation, and utilize the various roles the government, international organizations, Internet companies, technology communities, private institutions, and individual citizens may have. China should promote network governance within the UN framework and 'do a better job of giving rein to the positive role of all kinds of non-state actors' (Xi, 2018).

China's 2016 *National Cyberspace Security Strategy* is a work guide

On 27 December, 2016, the China National Internet Information Office released China's first *National Cyberspace Security Strategy* (CNIIO, 2018). The strategy, which was widely recognized around the world, defines cyberspace as a new channel for information dissemination, a new space for production and life, and a new engine for economic development and culture. It is also a new carrier of prosperity, a new platform for social governance, a new bond for exchanges and cooperation, and a new frontier for national sovereignty. The strategy has enriched and perfected the ideas of 'network sovereignty' advocated by China, and proposed that the Chinese government aim for peace, security, openness, cooperation and order in cyberspace. China is determined to handle the relationship between security and development. The content of the information infrastructure, showing cooperation and opening up to the international community, is the basic principle underlying network security in China, and it also shows China's sense of responsibility in firmly maintaining cyberspace security. The strategy proposes the direction and strategic tasks for China to maintain cybersecurity in the coming period, including: i) firmly defending cyberspace sovereignty; ii) resolutely safeguarding national security; iii) protecting critical information infrastructure; and iv) strengthening the construction of online culture; v) combating cyber terrorism, law-breaking and crime; vi) improving the network governance system; vii) consolidating the network security foundation; viii) enhancing the cyberspace protection capability; and ix) strengthening international cooperation in cyberspace.

New, emerging, threats to Chinese cybersecurity

In March 2018, China changed the original central cybersecurity and informatization leading group into the Central Committee for Cybersecurity and Informatization of the Communist Party of China. This is currently the highest institution, which will in the future lead China's cybersecurity work. Other departments of the Chinese government, such as the Ministry of Public Security, the Ministry of Industry and Information Technology, and the State Internet Information Office, are responsible according to their respective functions. The primary unit responsible for monitoring and maintaining the technical security and functionality of the Chinese cyberspace is the China Internet Emergency Response Center (CNCERT).

Recently, China's cyber security situation has had the following characteristics: first, the conventional network threats faced have been slightly reduced. According to CNCERT monitoring, the level of conventional Trojans, viruses, and botnets has declined. The United States, Hong Kong, Russia, Taiwan, and Japan are key countries and regions from which cyber-attacks are expected to emanate, and these need to be guarded against. Second, network security vulnerabilities continue to increase. Third, the malicious threat faced by Chinese industrial control systems (SCADA) deserves high vigilance. Fourth, there have been some major cybersecurity incidents in China. For example, the Cisco High-Risk Vulnerability CVE-2018-0171 was used by hackers and damaged many organizations in China. Fifth, the APP application has damaged users' personal information. Some mobile applications in the Chinese market have problems such as unutilized collection and the use of user information, a failure to fulfil security protection obligations, etc., and they endanger user information security. Sixth, user data leakage incidents have occurred across the Internet – in logistics, hotel and other industries – with up to hundreds of millions of information records being suspected of being implanted with malicious programs through data terminals, and internal security management mechanisms are not perfect. Seventh, the cloud computing platform

has repeatedly failed, and there are problems such as large-scale user access abnormalities and user data loss. Finally, ransomware has seriously compromised the legitimate rights and interests of network users – GlobeImposter and WannaCry ransomware attacks have occurred throughout China (CNCERT, 2019).

Maintaining network security as a core policy direction

Currently, China's network security workstations are at a new starting point. To predict the direction of China's cybersecurity policy in the future, we must consider the following aspects:

First, establishing cybersecurity as a wide security concept encompassing and involving all areas of national security. Therefore, maintaining network security should be the starting point for implementing the overall national security concept. However, unlike the 'network deterrent' approach of the United States (DoD, 2018; Lewis, 2020), China is determined to strengthen international cooperation and advocate sharing and co-governance under the concept of the 'community of cyberspace destiny' and in the spirit of 'common security'. Moreover, China is focusing on combatting cybercrime, building a clear network space, and strengthening global cyberspace governance with Chinese characteristics.

Second, in the Nineteenth National Congress report of the Communist Party of China, there have been new expressions and new requirements for informationization and cybersecurity work (Xi Jinping, 2017). It needs to be implemented in the future network security work and completed through new policy measures.

Third, the cyberspace security situation has undergone new changes. In particular, China's current critical information infrastructure is facing a sharp increase in attacks. China may face major national cybersecurity attacks, while China's cyber defence capabilities are still weak and the defensive side is still expanding. At the same time, the competition for data around the various actors in cyberspace, including national governments, will be unprecedentedly fierce. Some giant information technology (IT) companies have the ability to get data and manipulate it. The Cambridge Analytics company is an example.

Fourth, network and information technology continue to develop, especially in the areas of the Internet of Things and artificial intelligence. New developments mean the emergence of new threats. For example, once a hacker uses artificial intelligence to attack, the consequences are terrible. Another example is the current digital currency trading platform, which is becoming more and more popular, where its high level of profits has attracted the attention of hackers. And, with the development of digital currency, more and more cyber-attacks will be attracted, which will lead to financial network security problems. To this end, all —countries continue to revise, improve, upgrade, and introduce their own cybersecurity strategies.

Security by design

Fifth, from the perspective of the IT industry, the concept of 'security by design', that emphasizes intentionally designed and inbuild safety features of IT products, will be promoted and emulated. That is, safety is a factor that must be considered at the beginning of product design. However, such products may not actually appear until 2019 or later. In this field, there is still a long way to go to define what kind of technical standards are to be implemented and how to ensure that the global supply chain will also develop in this direction in the future. Since China is a global powerhouse in manufacturing IT products, and increasingly a designer, too, ensuring products on the international and domestic markets are safe and reliable is of paramount of importance.

International cooperation

China should take the ‘Belt and Road Initiative’ as an opportunity to strengthen cooperation with countries along the route, especially developing countries, in areas such as basic network infrastructure construction, the digital economy, cybersecurity, and build a Digital Silk Road for the twenty-first century (CNIIO, 2016; Xi, 2018). Here, China has both an opportunity and a historical opportunity, or even responsibility, for improving the cybersecurity of developing countries.

Civil-military integration

Seventh, absorb the experience of other countries and do a good job of military and civilian integration in the field of cyber security. China has noted that the integration of cyber security into both the military and the civilian population is an internationally accepted method. For example, the United States has established a network security strategy system covering government, military, and private enterprises, and has formulated relatively complete cyber security laws, regulations, policies, and standards, forming a joint government and military leadership, with the participation of multinational IT companies and the coordination of social organizations. There is cooperation in the national network security system. In accordance with Prime Minister Abe’s security-centric agenda, the Japanese government has launched a programme to spur innovation and the employment of dual-use technologies. The purpose is to enable the New Energy and Industrial Technology Development Organization (NEDO) to identify suitable new technologies and innovations which Japanese industry could then turn into civilian and military products for domestic and foreign customers (Reuters, 2015). Through policy measures, the Russian government also encourages the expansion of its network security military-civilian integration development space (RU MFA, 2016). President Xi Jinping, too, has stressed the strengthening of civil-military integration in the cybersecurity and informatization domain (CGTN, 2017; Xi Jinping, 2018).

At present, maintaining cyberspace sovereignty, protecting the country’s key information infrastructure, and protecting the security of citizens’ personal data are the three major priorities for China’s cybersecurity work. At the same time, China will gradually build and form its own network deterrent capability, while strengthening international cooperation. It will form an effective deterrent against criminals, terrorist organizations and countries and groups that are arrogant in cyberspace, and maintain peace in cyberspace. The key words are: safe and stable; safety and stability; international peace and security.

References

- CGTN (2017) China names key areas of military-civilian integration. Available from: <https://news.cgtn.com/news/7741444d30517a6333566d54/index.html> [accessed 18 July 2019].
- China National Internet Information Office (CNIIO) (2016) *National Cyberspace Security Strategy*. Available from: <https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/> [accessed 17 June 2019].
- Department of Defense (DoD) (2018) *Summary. Department of Defense Cyber Strategy*. Available from: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf [accessed 3 June 2019].
- Lewis, J. (2020) Risk, resilience and retaliation: American perspectives on international cybersecurity. In Tikkanen, E. and Kerttunen, M. (eds) *Routledge Handbook of International Cybersecurity*. Abingdon, Routledge.

- National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT) (2019) Weekly reports. Available from: www.cert.org.cn/publish/english/115/index.html [accessed 17 June 2019].
- Reuters (2015) Exclusive: Japan civilian R&D agency to get military role to spur arms innovation – sources. (20 March) Available from: www.reuters.com/article/us-japan-r-d-military-idUSKBN0MF2K520150320 [accessed 18 September 2019].
- The Ministry of Foreign Affairs of the Russian Federation (RU MFA) (2016) Doctrine of Information Security of the Russian Federation. 646 (December 5).
- The White House (2018) *National Cyber Strategy of the United States of America*. Available from: www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [accessed 15 June 2019].
- Xi Jinping (2017) Secure a decisive victory in building a moderately prosperous society in all respects and strive for the great success of socialism with Chinese characteristics for a new era. Speech 19th National Congress of the Communist Party of China (October 18) Available from: www.chinadaily.com.cn/china/19thcpnationalcongress/2017-11/04/content_34115212.htm [accessed 15 June 2019].
- Xi Jinping (2018) Speech at the National Cybersecurity and Informatization Work Conference. (20 April) Translation of Xinhua News Agency report. Available from: www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/ [accessed 17 June 2019].

Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

PART IV

Global approaches to cybersecurity

Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

24

CYBER DIPLOMACY

An Australian perspective

Tobias Feakin and Johanna Weaver

Introduction

The Secretary-General of the United Nations, Antonio Guterres, has appropriately asked,

When future generations look back at our times, I believe they will ask three questions: Did you work to preserve our planet from climate catastrophe? Did you make and keep the peace? And did you ensure that the digital age was one of prosperity and fulfilment? *(Guterres, 2019).*

Cyber, digital and technology issues now infuse almost every aspect of foreign policy. Once considered niche issues of technical concern, they are now incontrovertibly and intrinsically linked to national security, international stability, global economic prosperity and sustainable development. As the world increasingly recognizes this strategic significance, it is incumbent on the growing community of cyber-savvy diplomats to ensure that domestic and international policy responses mitigate the associated risks, while harnessing the opportunities and not inadvertently limiting the benefits of the digital age. Have we worked to keep the peace and ensure digital prosperity?

Australia's International Cyber Engagement Strategy (GoA, 2017c) set an ambitious agenda. Covering the full spectrum of cyber, digital and technology issues (collectively defined as 'cyber affairs'), the Strategy laid out the Australian Government's plans to engage internationally to:

- maximize opportunities for economic prosperity through digital trade;
- foster a strong and resilient cyber security posture;
- improve cybercrime prevention, prosecution and cooperation;
- promote a stable and peaceful online environment;
- strengthen multi-stakeholder Internet governance;
- support respect for human rights and democratic principles online; and
- encourage responsible use of digital technologies to achieve inclusive and sustainable development.

Two years after its publication, these principles, interests and goals remain current. We have made considerable progress towards implementation of the 61 actions in the Strategy's Action Plan (GoA, 2019b). This article reflects on the evolution of cyber affairs as a domain of diplomacy and foreshadows priority areas for engagement in the near to medium term.

Cyber affairs as a domain of diplomacy

When Australia's inaugural Ambassador for Cyber Affairs, Dr Tobias Feakin, took office in January 2017, his position was one of a few of its kind in the world. Today, many countries have dedicated teams within foreign ministries working on strategic cyber issues, for example, including but not limited to: Australia, Brazil, Canada, Cambodia, China, Denmark, Estonia, European External Action Service, Finland, France, Germany, India, Indonesia, Italy, Japan, Kenya, Korea (Republic of), Mexico, Morocco, the Netherlands, New Zealand, Norway, Poland, Russia, Singapore, South Africa, Switzerland, United Kingdom, and the United States. Of note, however, many of these teams continue to focus predominately on the international security dimensions of cyber diplomacy. It is a measure of maturity when foreign ministries and governments address cyber, digital and technology issues holistically.

Mitigating the risks and harnessing the opportunities are two sides of the same coin. In today's interconnected world – and more so than ever before – domestic decisions have global implications and vice versa. To reflect these realities, careful calibration of policy is required. There are two complementary steps countries can take to facilitate this. First, expand the mandate and coordination function of existing teams within Foreign Ministries (see below for Australian examples). Second, mainstream consideration of these issues across government by up-skilling diplomats and policymakers on strategic cyber, digital and technology topics as, for example, Australia has done through development and delivery of a Cyber Affairs Diplomatic Academy curriculum.

Australia's Ambassador for Cyber Affairs has the mandate to coordinate Australia's international cyber engagement across Government. Upon commencement in January 2017, one small section within Australia's Department of Foreign Affairs and Trade (DFAT) supported the Ambassador for Cyber Affairs. As at June 2019, three dedicated sections within DFAT support the Ambassador for Cyber Affairs, representing a four-fold increase in staff. Reflecting the whole of government mandate, this team works closely with colleagues across DFAT and the Australian Government (including, routine coordination with 13 Australian Government agencies and departments).

Of course, getting our own respective houses in order is one thing but, to be genuinely effective, we also need to support others to do the same. Given the interconnected nature of cyberspace, cyber capacity building assistance directly benefits both the recipient and donor countries.

Investment in *Australia's Cyber Cooperation Program* has increased from an initial \$4 million over four years to \$34 million out to 2023. In addition, Australia has a \$14 million cyber security partnership with Papua New Guinea. Combined, this represents a twelve-fold increase in Australian funding – all of which is dedicated to practical projects to deliver on the goals set out in *Australia's International Cyber Engagement Strategy*. Our words are backed up by action.

As technologies integrate more and more into every aspect of life, it is likely that 'cyber diplomacy' will simply become 'diplomacy'. However, regardless as to whether these issues are managed by dedicated teams within DFAT, or increasingly officers throughout the

department, it is clear that cyber, digital and technology issues will continue to be central tenets of Australia's foreign policy well into the future.

What's next: challenges and opportunities

In the next year, Australia's international cyber engagement will focus on reaffirming clear expectations for responsible behaviour in cyberspace, increasing transparency and reducing impunity in cyberspace, uplifting global cyber capacity – all with a clear eye on the future of emerging and evolving digital technologies.

Reaffirming clear expectations

Clear expectations facilitate predictability, which in turn fosters stability. It is common to hear calls for 'new' international frameworks to respond to the 'new' challenges of the digital age. However, in most instances, the core principles and values of existing frameworks remain sound. Our task will be much simpler, quicker and effective if we renovate these existing frameworks, rather than demolish and rebuild them from scratch. This applies to almost all aspects of Australia's cyber affairs agenda.

For example, Australia is committed to actively shaping global rule-making on digital trade, including in trade agreement negotiations and through the Australian-led World Trade Organization E-commerce initiative. These trade rules support existing global and regional norms, principles and guidelines. Likewise, Australia recognizes that human rights apply online, just as they do offline. We do not need to rewrite these core principles, although we may need to develop specific tools to respond to the unique characteristics of the online environment.

Governments and citizens are increasingly focused on the need to be clear about expectations of responsible behaviour for the private sector and, in particular, technology companies. Gone are the days when regulation of cyberspace was dismissed as an impossibility (cf. Barlow, 1996; Government of New Zealand and Government of France, 2019; Zuckerberg, 2019). Like all actors, the private sector has rights – but it also has obligations. Governments need to develop incentives and, when necessary, legal sanctions to minimize harm to citizens, while preserving the many benefits of the Internet and digital technologies. This balancing act – between openness, freedom and security – is not new, but the global nature of cyberspace brings fresh challenges. We discuss this further in the section below on emerging and evolving technologies.

Clear expectations for responsible behaviour by states in cyberspace are also important. As observed by Australia's Foreign Minister, Marise Payne, '2019 will be a pivotal year in the development of the rules of the road in cyberspace. Two key UN bodies will meet this year to further strengthen the international framework that governs [state behaviour] in cyberspace' (Payne, 2019). Positively, these two Groups – a sixth United Nations (UN) Group of Governmental Experts (UNGGE) and an inaugural UN Open Ended Working Group (OEWG) – have strong foundations upon which to build.

In 2013, and again in 2015, all UN Member States agreed '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' (A/68/98; A/RES/68/243; A/70/174; A/RES/70/237). This seminal conclusion (contained in the 2013 report of the UNGGE (A/68/98), and reaffirmed in the 2015 report of the UNGGE (A/70/174)), was considered and endorsed, by consensus, by all members of the

UN General Assembly (A/RES/68/243 and A/RES/70/237). This represented a significant step forward – progressing the conversation from ‘if’ international law applies, to ‘how’ it applies to state conduct in cyberspace. The next step is continuing to deepen and refine common understandings on how particular legal principles apply to specific circumstances. This is not a challenge unique to the application of international law to cyberspace; international law is complex and its application raises complex questions in many fields, including state conduct in cyberspace. The OEWG and GGE provide an opportunity for all countries to put their views on the table. States also have the opportunity to annex their opinions on the application of international law to cyberspace to the UNGGE’s report. More generally, to foster common understandings, Australia encourages all states to publish their views on the application of international law to cyberspace, as we have done (GoA, 2017a; 2019).

In 2015, UN member states also endorsed a set of 11 norms of responsible state behaviour (A/70/174; A/RES/70/237). These norms largely reflected existing state practice. By capturing the norms in the UNGGE report, UN members set clear expectations of what countries should do, or refrain from doing, in cyberspace – with a view to promoting international peace and stability. For example, that states should take appropriate measures to protect critical infrastructure from ICT threats (op. cit., 13(g)) and refrain from ICT activity that intentionally damages critical infrastructure that provides services to the public (op. cit., 13(f)).

These norms complement existing international law and – combined with confidence building measures and coordinated capacity building – provide a clear framework for responsible state behaviour in cyberspace. The UN General Assembly considered and endorsed, by consensus, the eleven norms of responsible state behaviour, calling on all states ‘to be guided in their use of ICTs by the recommendations of the 2015 GGE Report’ (A/RES/70/237). Moreover, many regional groups and leaders’ meetings have also endorsed the 11 norms (see, for example, G20 2015, ASEAN Leaders Statement 2018; ASEAN Communications Ministers 2018; EAS Leaders Statement 2018; CHOGM Declaration 2018).

Active engagement in both the UNGGE and OEWG will be a priority for Australia’s cyber affairs team. Our objective is to deepen understanding of what states have already agreed at the UN – and bust, once and for all, the myth that cyberspace is a legal vacuum. We will work with both UN groups to provide practical guidance to states on how to implement these existing obligations (to engender compliance by all states, all of the time) and discuss coordinated capacity building (to ensure all countries are equipped to implement the agreed rules of the road). The reports of the UNGGE, endorsed by the UN General Assembly (op. cit.), are not just pieces of paper to Australia. Australia has publicly committed to act in accordance with these reports (see, for example, GoA, 2017c: p. 49). We walk the walk, not just talk the talk. And we expect others to do the same.

Increase transparency and reduce impunity in cyberspace

Australia’s efforts at the UN to reinforce the rules in cyberspace go hand in hand with our efforts to increase transparency and reduce impunity. While transparency among states differs significantly, it is undeniable that more and more countries are developing offensive cyber capabilities. The five permanent members of the United Nations Security Council have publicly declared offensive cyber capabilities, and several other countries have declared, or are thought to be developing, offensive cyber capabilities (see, for example, Lewis and Timlin, 2011; Council of Foreign Relations, 2019; GIP Digital Watch, 2019).

Australia recognizes the legitimate right of states to develop these capabilities. Indeed, Australia has publicly declared that we have offensive cyber capabilities, and that we use them. Then Prime Minister Turnbull first disclosed the capabilities in 2016 (GoA, 2016, p. 28; Turnbull, 2016) and as noted by Mike Burgess, Director-General of the Australian Signals Directorate,

Since then, further announcements have established how the capability supports the ADF – including military operations in the Middle East where offensive cyber operations have helped disrupt Daesh’s ability to communicate, launch attacks and spread propaganda. The government has also revealed the role the capability plays in disrupting foreign cybercriminals that target Australians.

(Burgess 2019)

Information on the conduct and authorization of offensive cyber capability in support of military operations was also published in Australia’s International Cyber Engagement Strategy (GoA, 2017c, p. 55)

The Australian Signals Directorate (ASD) has ‘come out of the shadows’. Transparency breeds accountability. As recognized by Mike Burgess, Director-General of ASD, “coming out of the shadows doesn’t mean that we will be able to talk about the detail of our operations. Some things will need to remain classified out of necessity” (Burgess, 2018). However, as Burgess made clear,

[r]egardless of the context, all our [ASD’s] operations are conducted in accordance with international and Australian law. Every mission must be targeted and proportionate, and is subject to rigorous oversight. All our actions are deeply considered, and subject to meticulous planning to consider the potential for unintended consequences. ASD takes its legal and ethical responsibilities incredibly seriously. We pride ourselves on being meticulous in execution. And we operate within the law.

(Burgess, 2019)

Australia’s acknowledgment of these capabilities does not contradict our commitment to a peaceful and stable online environment. Instead, it sends an unambiguous message that states’ activities in cyberspace have limitations and are subject to obligations, just as they are in the physical domain. Australia urges all countries likewise to be transparent about the development and use of these capabilities and unequivocal in their commitment to do so in accordance with domestic and international law, as well as norms of responsible state behaviour agreed at the UN.

Cyber risk remains in the high-impact, high-likelihood quadrant of the global risks landscape (World Economic Forum, 2019). There are many malicious actors in cyberspace. However, if – like Australia – all states acted in accordance with agreements made at the UN, the risk of a cyber incident with the potential to undermine international peace and stability would be significantly reduced.

We have agreed the rules of the road for states in cyberspace; we now need to ensure all states abide by them. States cannot act in cyberspace with impunity. With this objective in mind, and in coordination with a growing number of international partners, Australia publicly attributed to the Democratic People’s Republic of Korea, Russia, Iran, and China malicious cyber activity that was inconsistent with international law or agreed norms of responsible behaviour (Government of Australia, 2017b, 2018e, 2018d, 2018c, 2018a, 2018b; Turnbull,

2018). In December 2017, Australia joined with five countries to attribute the WannaCry ransomware campaign to DPRK. In February 2018 when Australia joined 11 countries to call out the NotPetya malware attacks on critical infrastructure and businesses to Russian state-sponsored actors. In March 2018, the FBI indicted Iranian-based actors; in August 2018 Prime Minister Turnbull declared that 33 Australian universities were targeted by an Iran-based spear-phishing campaign as part of a sophisticated attempt to steal intellectual property and academic research. In April 2018, Australia joined the US and UK to attribute the worldwide targeting of Cisco routers to Russian state-sponsored actors. In October 2018, Australia joined 21 international partners to call out Russia for a pattern of malicious cyber activity targeting political institutions, businesses, media, and sport. In October 2018, the Foreign Minister also condemned Russian cyber operations against the Organization for the Prohibition of Chemical Weapons (OPCW) and flight MH17 investigation. In December 2018, Australia joined with 13 countries to call out a global campaign of cyber-enabled intellectual property theft to a group known as APT10, acting on behalf of China's Ministry of State Security.

When it is in our interests to do so, Australia will continue to participate in internationally coordinated public attributions. However, public attribution is not the only tool in our tool kit.

In 2018, the Australian Government conducted a comprehensive stocktake of available response options to unacceptable behaviours in cyberspace. The Review encompassed diplomatic, economic, legal, and law enforcement, defence-based, and private sector measures. The Review's findings will shape Australia's responses to significant cyber incidents. Australia's response will always be proportionate to the circumstances of the incident, will comply with domestic law, and be consistent with our support for the rules-based international order and our obligations under international law.

In responding to malicious activity, Australia and our international partners seek to engender greater compliance with the rules and norms agreed at the UN. Our objective is to preserve and promote a peaceful and stable online environment for the benefit of all.

Uplift global cyber capacity

Australia acknowledges that not all countries are equally positioned to benefit from the digital age – and we are taking practical action to address this imbalance. Our \$34 million Cyber Cooperation Program aims to equip countries in ASEAN and the Pacific with the capacity to respond to the challenges and harness the opportunities of increased connectivity. The Program has five areas of focus, namely:

1. International cyber stability framework: promoting an understanding of how existing international law, norms and confidence building measures apply in cyberspace.
2. Cybercrime prevention, prosecution and cooperation: strengthening legislative frameworks and institutional capacity to prevent, investigate and prosecute cybercrime.
3. Cyber incident response: working with partners to establish and strengthen national and regional cyber incident response capability and coordinate and share cyber security threat information across the region.
4. Best practice technology for development: advocating for best practice use of technology for development by integrating cyber security by design and respect for human rights online.
5. Human rights and democracy online: advocating and protecting human rights and democracy online, including freedom of expression online.

As stated above, Australia also has a \$14 million Cyber Security Partnership with Papua New Guinea, which complements our Coral Sea Cables Project (in partnership with the Solomon Islands and Papua New Guinea) and the expansion and upgrade of a satellite ground station in Port Moresby.

More broadly, Australia's aid program supports increased access to, and innovative uses of, digital technologies to drive sustainable and inclusive development. We are drafting guidance to ensure that human rights online are protected, and that all digital technologies used in, or provided to, Australian aid and non-government projects are secure by design.

Many countries, and increasingly non-government organizations, are also developing capacity building programs. For example: the Global Forum of Cyber Expertise (GFCE) has 67 members comprising countries, intergovernmental organizations (IGOs), international organizations, and private companies with the commitment to contribute to cyber capacity building. For Australia, a key objective in the near term is seeking practical ways to better coordinate the delivery of these programmes across governments, civil society, academia, and the private sector. In doing, so we will ensure our combined resources, networks and expertise will be a force multiplier in pursuit of shared goals.

These activities demonstrate Australia's commitment to the United Nations 2030 Agenda for Sustainable Development, which recognizes the vital role of digital technologies to achieve a better and more sustainable future for all.

Clear eye on the future: emerging and evolving technology

We live in the most interconnected era in history. Activities online already have a direct impact on our experiences in the physical world. With the assimilation into our daily lives of artificial intelligence, quantum computing, advanced integrated circuits, fifth generation, '5G', mobile technologies, and the Internet of Things (IoT), the distinction between online and offline will become increasingly intertwined and, in the not too distant future, entirely interdependent.

In his seminal text *Code 2.0*, Lessig (2006), compelled all users of technologies to 'learn at least enough to see that technology is plastic. It can be [made and] remade differently.... We should expect – and demand – that it can be made to reflect any set of values that we think important' (p. 32).

Just as humans designed and built the Internet, many of the brightest minds in the world are currently grappling with the design and development of these new, emerging and evolving technologies. These technologies will shape the way we interact – online and offline – as individuals, as organizations, and as countries. It would be remiss of us not to demand that these technologies be made to reflect values we – as individual and as countries – think are important. Likewise, it would be naïve of us not to be prepared for others to have differing views. This brings us full circle, demonstrating the need for a cadre of tech-savvy diplomats attuned to these sensitivities and equally able to pursue Australia's interests with technologists and the private sector as with other governments.

Conclusion

The Australia government has been an early adopter and strong supporter of cyber diplomacy. Our starting point – across the full spectrum of cyber affairs – is not that we need to develop new frameworks, but rather that the rules from the 'real' world should apply online. Individuals, organizations and countries should enjoy the same protections

and freedoms online as we do offline. Australia will continue to champion an open, free, and secure cyberspace that protects national security, promotes international stability, while driving economic growth and sustainable development. In doing so, we will preserve a peaceful and stable online environment for the benefit of all.

References

- Barlow, J.P. (1996) *A Declaration of the Independence of Cyberspace*, Electronic Frontiers Foundation. Available at: <https://projects.eff.org/~barlow/Declaration-Final.html> [accessed 19 November 2015].
- Burgess, M. (2018) *Speech to ASPI National Security Dinner: Then and Now – Coming Out from the Shadows*. Available at: www.asd.gov.au/speeches/20181029-aspi-national-security-dinner.htm [accessed 27 June 2019].
- Burgess, M. (2019) *Speech to the Lowy Institute*. Available at: www.asd.gov.au/speeches/20190327-lowy-institute-offensive-cyber-operations.htm [accessed 27 June 2019].
- Council of Foreign Relations (2019) *Cyber Operations Tracker*. Available at: www.cfr.org/interactive/cyber-operations [accessed 27 June 2019].
- GIP Digital Watch (2019) *Offensive Cyber Capabilities*. Available at: <https://dig.watch/processes/un-gge> [accessed 27 June 2019].
- Government of Australia (GoA) (2016) *Australia's Cyber Security Strategy*. Available at: <https://cybersecuritystrategy.homeaffairs.gov.au>.
- Government of Australia (GoA) (2017a) *Annex A: Australia's position on how international law applies to state conduct in cyberspace, Australia's International Cyber Engagement Strategy*. Available at: www.dfat.gov.au/aices [accessed 27 June 2019].
- Government of Australia (GoA) (2017b) *Attribution of WannaCry to DPRK, Media Release*. Available at: <https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/australia-attributes-wannacry-ransomware-to-north-korea.pdf> [accessed 27 June 2019].
- Government of Australia (GoA) (2017c) *Australia's International Cyber Engagement Strategy*. Available at: www.dfat.gov.au/aices [accessed 24 June 2019].
- Government of Australia (GoA) (2017d) *Australian Cyber Security Centre 2017 Threat Report*. Available at: www.cyber.gov.au/sites/default/files/2019-03/ACSC_Threat_Report_2017.pdf [accessed 27 June 2019].
- Government of Australia (GoA) (2018a) *Attribution of a Pattern of Malicious Cyber Activity to Russia, Media Release*. Available at: <https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/attribution-of-a-pattern-of-malicious-cyber-activity-to-russia.pdf> [accessed 27 June 2019].
- Government of Australia (GoA) (2018b) *Attribution of Chinese Cyber-Enabled Commercial Intellectual Property Theft, Media Release*. Available at: <https://dfat.gov.au/international-relations/themes/cyber-affairs/Pages/attribution-of-msps-cyber-intrusions.aspx> [accessed 27 June 2019].
- Government of Australia (GoA) (2018c) *Attribution of Malicious Cyber Activity to Russia, Media Release*. Available at: <https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/australia-condemns-cyber-operations-attributed-to-russia-targeting-opcw.pdf> [accessed 27 June 2019].
- Government of Australia (GoA) (2018d) *Australian Government Attribution of Cyber Incident to Russia, Media Release*. Available at: <https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/australia-attributes-cyber-incident-to-russia.pdf> [accessed 27 June 2019].
- Government of Australia (GoA) (2018e) *Australian Government Attribution of the 'NotPetya' Cyber Incident to Russia, Media Release*. Available at: <https://dfat.gov.au/international-relations/themes/cyber-affairs/Documents/australia-attributes-notpetya-malware-to-russia.pdf> [accessed 27 June 2019].
- Government of Australia (GoA) (2019a) *2019 International Law Supplement, Australia's International Cyber Engagement Strategy*. Available at: www.dfat.gov.au/aices [accessed 27 June 2019].
- Government of Australia (GoA) (2019b) *International Cyber Engagement Strategy, 2019 Progress Report*. Available at: www.dfat.gov.au/aoces [accessed 27 June 2019].
- Government of New Zealand and Government of France (2019) *Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online*. Available at: www.christchurchcall.com/ [accessed 26 June 2019].
- Guterres, A. (2019) *Remarks to Informal Meeting of the General Assembly on the Independent High-Level Panel on Digital Cooperation*. Available at: www.un.org/sg/en/content/sg/speeches/2019-06-10/independent-high-level-panel-digital-cooperation-remarks-general-assembly [accessed 24 June 2019].

- Lessig, L. (2006) *Code: Version 2.0*. New York: Basic Books.
- Lewis, J.A. and Timlin, K. (2011) *Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization* Center for Strategic and International Studies. Available at: <http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf> [accessed 27 June 2019].
- Payne, M. (2019) *Address to the Lowy Institute*. Available at: https://foreignminister.gov.au/speeches/Pages/2019/mp_sp_190311.aspx [accessed 26 June 2019].
- Turnbull, M. (2016) *Launch of Australia's Cyber Security Strategy*. Available at: <https://pmtranscripts.pmc.gov.au/release/transcript-40308> [accessed 27 June 2019].
- Turnbull, M. (2018) *Speech at the opening of the Australian Cyber Security Centre*. Available at: www.malcolmturnbull.com.au/media/speech-at-the-opening-of-the-australian-cyber-security-centre-canberra-16-a [accessed 27 June 2019].
- United Nations General Assembly (UNGA) (2013) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/68/98 (24 June).
- United Nations General Assembly (UNGA) (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174 (22 July).
- United Nations General Assembly (UNGA) (2014) *Resolution adopted by the General Assembly on 27 December 2013, Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/68/243 (9 January).
- United Nations General Assembly (UNGA) (2015) *Resolution adopted by the General Assembly on 23 December 2015, Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/70/237 (30 December).
- World Economic Forum (2019) *The Global Risks Report 2019*, 14th edition. Available at: <http://wef.ch/risks2019> [accessed 14 April 2019].
- Zuckerberg, M. (2019) *Four Ideas to Regulate the Internet*, Facebook Newsroom. Available at: <https://newsroom.fb.com/news/2019/03/four-ideas-regulate-internet/> [accessed 26 June 2019].

CONFIDENCE-BUILDING MEASURES IN CYBERSPACE

New applications for an old concept

Paul Meyer

In considering the current international discussion concerning state conduct in cyberspace the concept of confidence-building measures (CBMs) is frequently invoked. International institutions like people are often most comfortable with ideas or practices that have been in their purview for some time. Leading multilateral inter-governmental organizations, such as the United Nations at the global level, as well as regional organizations, notably the Organization for Security and Cooperation in Europe (OSCE), have considerable experience with CBMs in the context of international security and it is not surprising that they have had recourse to them in addressing radically new forms of problematic state behaviour in the cyber sphere.

In this chapter, I examine the origins of CBMs in the Cold War context in which they first emerged and consider the security objectives they were meant to achieve. The application of CBMs to the challenges presented by inter-state cyber operations will then be discussed including the key stages in their diplomatic development, notably by the UN and the OSCE. The chapter concludes with some observations as to the prospects for further development and implementation of CBMs in the context of international cyber security and against a backdrop of rising geopolitical tensions.

The origins of CBMs

The acute, massive armed confrontation of the Cold War period provided the crucible for CBMs. The opposing military camps of NATO and the Warsaw Pact with their forward deployed forces in the centre of Europe gave rise to concerns about the danger of surprise attack (especially amongst Western states which considered that the Soviet Union and its allies held a major advantage in conventional forces that could be employed in such an attack). These concerns underlaid the discussions in the security track of the Conference on Security and Cooperation in Europe (the predecessor of today's OSCE) which was a multi-faceted effort in keeping with the *détente* policy of the day to formulate a cooperative security order for Europe (and the transatlantic partners of the United States and Canada). The concept of CBMs as a means of reducing the risk of war took hold at that time and formed part of the *Helsinki Final Act* of 1975 which concluded these negotiations.

In the preambular paragraphs of the section of the *Final Act* dealing with CBMs, these measures are conceived as part of the effort to eliminate ‘the causes of tension that may exist among them’. In particular the document states:

Recognizing the need to contribute to reducing the dangers of armed conflict and of misunderstanding or miscalculation of military activities which could give rise to apprehension, particularly in a situation where the participating States lack clear and timely information about the nature of such activities.

(OSCE, 1975, p. 10)

The document proceeds to set out a few measures relating to prior notification of military manoeuvres and exchange of observers and affirms that such steps are important ‘for the promotion of mutual understanding, and the strengthening of confidence, stability and security’ (p. 11). Even at this early stage the measures were viewed as helping to prevent misunderstanding or miscalculation on the part of opposing militaries that could be destabilizing and potentially lead to armed conflict.

Within the OSCE context over subsequent years, the modest initial set of CBMs were elaborated on and extended through a series of new arrangements (while retaining their politically-binding nature), under the rubric of the *Vienna Document on Confidence and Security Building Measures* starting in 1990 and continuing until the current version agreed on in 2011. The insertion of the term ‘security’ was to underline that these measures were to have military/security significance beyond the goal of confidence-building. Alongside the *Treaty on Conventional Forces in Europe* (CFE) and *The Open Skies Treaty* these arrangements were considered by the OSCE to ‘ensure predictability, transparency and military stability and reduce the risk of a major conflict in Europe’ (OSCE, 2011).

The UN takes up CBMs

Although CBMs first emerged in the European context and under the auspices of the CSCE and later the OSCE they were also the subject of scrutiny at the universal level of the UN. Through the mechanism of a UN Group of Governmental Experts (GGE), a body of government nominated experts normally consisting of 15–25 representatives who are tasked with studying a given issue and preparing a consensus report if agreed, the subject of CBMs was also considered. Pursuant to a UN General Assembly resolution of 1979 (34/87B), a GGE under the chairmanship of Ambassador Gerhard Peiffer of Germany, considered CBMs and produced a consensus report in October 1981 (UNGA, 1981).

The Secretary-General’s forward to the GGE report indicated that ‘CBMs aim at strengthening international peace and security and at fostering a climate of trust and international cooperation among states in order to facilitate progress in the disarmament field’ (UNGA, 1981, p. 3). Although rooted in international security and in particular the subset of arms control and disarmament, the GGE took an expansive view of the role of CBMs suggesting that ‘the goal of CBMs is to contribute to, reduce or, in some instances, even eliminate the causes for mistrust, fear, tensions and hostilities, all of which are significant factors in the continuation of the international arms build-up’ (p. 11). The conflict prevention potential of CBMs was stressed in the GGE report:

one of the main objectives of CBMs must be to reduce the elements of fear and speculation in order to achieve a more accurate and more reliable reciprocal assessments

of military activities and other matters pertaining to mutual security, which cause mutual apprehensions and increase the danger of conflict.

(p. 12)

The theme of greater clarity about capabilities and intentions leading to greater stability was also salient in the report, which even cited the establishment of the 'hot line' between the USSR and the USA in 1963 as an initial CBM that should be emulated: 'appropriate CBMS such as adequate communication channels, including 'hot lines' should be provided especially in situations of crisis where they can have an important stabilizing effect and improve existing instruments of international crisis management' (p. 15).

Interestingly, given the voluntary, politically-binding status of the existing CBMs that had been adopted by the CSCE, the GGE report expressed a clear preference for legally-binding measures: 'As soon as possible voluntary measures should accordingly be developed into politically binding provisions and politically-binding provisions changed into legally-binding obligations' (p. 34).

The UN addresses international cyber security policy: first steps

The earlier UN work on CBMs did not have immediate relevance to the new technological phenomenon of the Internet and the wider concept of cyberspace (the UN has formally adhered to the descriptor of 'information and communication technologies' or ICTs). However, in 1998 at the initiative of the Russian Federation, the issue of cyber activity and international security was placed on the agenda of the UN General Assembly and its First Committee (Disarmament and International Security). Its resolution, entitled *Developments in the Field of Information and Telecommunications in the Context of International Security* was first adopted by the General Assembly in the fall of 1998 and has been a perennial presence under the same title, albeit with expanding content, at the First Committee ever since.

Although this initial resolution concentrated (as did much early UN cyber-related work) on combatting potential exploitation of ICT for criminal or terrorist purposes, it did squarely raise the spectre of these technologies as a potential threat to international security. In a preambular paragraph the resolution expresses 'concern 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 security of States' (UNGA, 1999).

Prompted by resolution 53/70 and the emergence of a new security issue, the UN Department of Disarmament Affairs and the UN Institute for Disarmament Research (UNIDIR), convened a private discussion in August 1999 of *Developments in the Field of Information and Telecommunications in the Context of International Security*. The summary of this discussion reveals a nascent awareness of the magnitude of the threat to international security as well as the difficulties in delineating the problem from a conventional arms control perspective. Picking up on some of the unique features of offensive use of ICTs the report flagged that 'it is difficult to identify attackers and to distinguish between electronic vandals at one end of the spectrum and State aggressors at the other' (UNIDIR, 1999). The report also noted the challenge of differentiating between military attacks utilizing advanced technologies (associated with the then current theme of the 'Revolution in Military Affairs') and 'information operations' observing that 'it is increasingly easy for states or groups to use propaganda, disinformation or psychological operations in order to achieve their strategic, political or economic goals' (p. 2).

The report's conclusion indicated considerable uncertainty as to whether 'information operations' could be legally employed or 'Should there be efforts to either control the proliferation of RMA/information operations capabilities or to restrict their use using the Laws of Armed Conflict?' (p. 4)

Getting greater clarity on some of these emerging questions was part of the motivation for the establishment, pursuant to UNGA resolution 58/32 of 8 December 2003, of the first UN GGE devoted to the international cyber security question. Under the chairmanship of Andrey Krutskikh of Russia, the GGE met in the 2004–2005 timeframe, but failed to reach consensus on a substantive report, due, in the words of the chairman, to 'the complexity of the issues involved' (UNGA, 2005a). A fuller account provided by the UN Office for Disarmament Affairs attributes the failure to a lack of consensus on 'whether or not to include language that stressed the new threats posed by State exploitation of ICTs for military and national security purposes'. The other stumbling block for consensus was 'whether the discussion should address issues of information content or whether it should focus only on information infrastructure' (UNODA, 2015).

The differences of view relating to whether military uses were to be addressed (and controlled in some manner) found expression in views of member states solicited by the Secretary-General pursuant to the resolution authorizing the GGE. The May 2004 submission of the UK for example rejected the need for any multilateral instrument

that would restrict the development or use of certain civil and/or military technologies. With respect to military applications of information technologies, such an instrument is unnecessary. The law of armed conflict, in particular the principles of necessity and proportionality, governs the use of such technologies.

(UNGA, 2004UK)

In a similar vein, the US submission stated 'With respect to military applications of information technology, an international convention is completely unnecessary. The law of armed conflict and its principles of necessity, proportionality and limitation of collateral damage already govern the use of such technologies' (UNGA, 2004US).

Not all countries providing their views to the Secretary-General were as sanguine about the military uses of ICT being a non-problem. Brazil's submission drew attention to the rise of 'cyber warfare', noting that 'Some armed forces are already deploying specialized military units, trained and equipped to disable or even destroy critical infrastructure by means of invasion and sabotage of information networks' (UNGA, 2005BR). Brazil also elaborated various cooperative measures that states could embrace including considering conventions on 'information warfare', but also the 'establishment of a code of conduct for the use of information weapons' (pp. 3–4). Although not employing the CBM term, these ideas, especially the proposal for a code of conduct, prefigure the type of CBMs that would eventually be promoted in the context of the UN GGEs.

The need to get ahead of the curve on this rapidly evolving security threat seemed to preoccupy some at UNIDIR who devoted an issue of *Disarmament Forum* to the theme of 'ICT and International Security' in which the Chair of the GGE, Andrey Krutskikh provided a 'special comment'. Foreshadowing the direction states were moving in, he wrote 'As states come to terms with the capabilities and dangers of information warfare, it is not implausible that a cyberspace arms race could erupt. Such a race would not only be immensely destabilizing, but would also ultimately divert enormous resources from peaceful and sustainable development' (UNIDIR, 2007, p. 2–3).

UN GGEs on international cyber security: CBMs emerge

The initial failure to achieve consensus with the 2004–2005 GGE did not dampen interest in pursuing the issues associated with cyber security operations. Already, at the 2005 General Assembly session, a resolution was overwhelmingly adopted authorizing the establishment in 2009 of a follow-on GGE ‘to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them’ (UNGA, 2005b).

This GGE, once more under the chairmanship of Ambassador Krutskikh, was able to agree on a substantive report delivered in July 2010. This report was explicit in noting the threat posed by state conduct in cyberspace and not just that of non-state actors. It referred to ‘increased reporting that States are developing ICTs as instruments of warfare and intelligence and for political purposes. Uncertainty regarding attribution and the absence of common understanding regarding acceptable State behaviour may create the risk of instability and misperception’ (UNGA, 2010). This language reflected the same concerns over the destabilizing potential of ‘misperception’ by states as had informed the earlier UN study of CBMs in a context of military confrontation. The GGE report recommended *inter alia* the development of ‘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’ (p. 8).

The elaboration of what these measures might look like was taken up by the next GGE established pursuant to a 2011 General Assembly resolution (66/24) that this time was adopted without a vote. Its mandate specifically included under the ‘cooperative measures’ rubric, ‘norms, rules or principles of responsible behaviour of States and confidence-building measures with regard to information space,’ (UNGA, 2011) Under the chairpersonship of Australian Ambassador Deborah Stokes, this GGE was also able to agree on a substantive report which was issued in June 2013. This report devoted an entire section to CBMs and information exchange and explicitly designated these as ‘voluntary, confidence-building measures’ [that] ‘can promote trust and assurance among States and help reduce the risk of conflict by increasing predictability and reducing misperception’ (UNGA, 2013). This was classic CBM language with its emphasis on promoting trust and reducing risk of conflict through increased transparency and predictability. The recommended CBMs were largely of the exchange of information type although they did include more operational measures that were directly linked to conflict prevention. Thus, the GGE called for ‘enhanced mechanisms for law enforcement cooperation to reduce incidents that could otherwise be misinterpreted as hostile State actions would improve international security’ (p. 9).

A further innovation of this GGE was the acknowledgment that other stakeholders should be involved in the work of CBM development. The report stated: ‘While States must lead in the development of confidence-building measures, their work would benefit from the appropriate involvement of the private sector and civil society’ (p. 10). In the event ‘appropriate involvement’ has been interpreted as very little, and the GGE process has remained essentially impenetrable to outside private sector or civil society inputs.

The apogee of GGE confidence building: the 2015 report

The momentum created by the successful GGE reports of 2010 and 2013 carried over to the 2014–2015 iteration of the GGE, with 20 state representatives participating under the chairmanship of Carlos Perez of Brazil. The consensus report issued by this group in July 2015 was viewed as the most elaborated set of recommendations to date, and, in view of what has occurred

subsequently, may be seen as an apogee of sorts for the UN GGE endeavour on international cyber security policy. The 2015 report conveyed a greater sense of what was at stake if cooperation was not strengthened and a sense of urgency in doing so. The report referred to

disturbing trends in the global ICT environment, including a dramatic increase in incidents involving the malicious use of ICTs by State and non-State actors. These trends create risks for all States, and the misuse of ICTs may harm international peace and security.

(UNGA, 2015)

In the inventory of potential remedial action to prevent this escalation of conflict, CBMs occupied a key place in the view of the GGE. From the initial sentences of its section on CBMs the 2015 report is clear in its evaluation of the worth of CBMs: ‘Confidence-building measures strengthen international peace and security. They can increase interstate cooperation, transparency, predictability and stability’ (p. 9). In order to realize the benefits of enhanced trust and a reduction in the risk of conflict the report recommended some 14 voluntary CBMs. They included such basic steps as the identification of points of contact and the development of consultative mechanisms at the bilateral, regional, sub-regional and multilateral levels to more ambitious measures such as cooperation amongst computer emergency response teams/cybersecurity incident response teams for ‘information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks, including co-ordinating responses’ (p. 10). Significantly, there were calls for states to share information on what they considered to be critical infrastructure and how best to address vulnerabilities in such infrastructure. This mirrored to a degree language in the ‘norms, rules and principles for responsible state behaviour’ section which specified 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’ (p. 8).

The distinctions between ‘norms, rules and principles’ on the one hand and CBMs on the other were always rather blurred in the GGE treatment of these ideas. Although both were recommended to states on a voluntary basis, there appeared to be some recognition that CBMs should be of more specific and operational nature, a means of putting into practice the ‘norms, rules and principles’ set forth in the reports. The fact that each concept was given a separate section in the GGE reports also suggests this functional distinction was considered important to retain.

The GGE process hits a snag: the failure of 2017 and the turmoil of 2018

The series of successive GGEs generating consensus reports came to an end with the failure of the 2016–2017 GGE, expanded to include 25 representatives, to agree on a final report. The proximate reason for this failure was disagreement over how international law is to apply to state cyber activity. A divide emerged between the US and Western allies on one hand and China and Russia on the other over whether explicit endorsement of the applicability of international humanitarian law to inter-state cyber operations should be given which presupposes that armed conflict in cyberspace would occur. In the words of one analyst, ‘Russian and Chinese diplomats wanted to concentrate their efforts on preventing cyber-based conflict in the first place, instead of setting the rules for something that should not be allowed to happen’ (Grigsby, 2017, p. 114).

This failure was also seen as reflecting the significant deterioration in geopolitical relations amongst the leading cyber powers of China, Russia and the US since the 2015 GGE outcome. As one analysis of the GGE failure concluded:

The outcome of the most recent GGE simply confirms that there are significant differences of opinion between states on how to apply international law to state use of ICTs, and there was not enough determination among the participating experts to overcome them.

(Tikk & Kerttunen, 2018, p. 22)

At a time when mistrust was growing and strategic consultative processes terminated or suspended, it was becoming more difficult to promote cooperative approaches to international cyber security and obtain traction for cyber CBMs although arguably this was when such measures were most needed.

If there were still hopes that the failure of the 2017 GGE could be overcome via a new GGE authorization, the developments at the 2018 General Assembly session served to dispel these.

Despite the fact that hitherto the resolutions establishing GGEs had enjoyed consensus status, the 2018 First Committee session of the General Assembly was presented with two competing resolutions setting out different future paths for UN work on cyber security. After years of supporting reiterations of the GGE format, Russia put forward a more ambitious resolution that foresaw the establishment in 2019 of an Open-Ended Working Group (i.e. one in which any interested UN member state could participate) to ‘further develop the rules, norms and principles of responsible State behaviour’ and to render a report by the fall of 2020. The resolution also incorporated selected elements from earlier GGEs (UNGA 2018). The US, for its part, championed a resolution authorizing a standard GGE in 2019 with a mandate to continue to study the issue of possible cooperative measures and to report back to the 2021 session of the General Assembly (UNGA, 2019). After years of leading on GGEs which remain opaque mechanisms limited to a few states, Russia was now stressing the ‘more democratic, inclusive and transparent’ nature of its Open-Ended Working Group proposal. The US was left to defend the traditional GGE formula, although in recognition of the frustration of some excluded member states, it incorporated a provision in its resolution for convening two open-ended informal consultative meetings during the term of the GGE.

In the normal conduct of First Committee business, the expectation would be for the two lead sponsors to make an effort to combine the two draft resolutions into a single variant in order to gain maximum support for it. The downturn in relations were such that compromises on the text were not in the event achieved and the First Committee was obliged to vote on the two competing resolutions. Despite the obvious disconnects between the two processes and the challenge it would represent for UN resources and policy coherence, both resolutions were adopted by the Assembly.

Although both resolutions referred to continued study of CBMs it is unclear how they will fare in this new bifurcated UN process. Some division of labour between these two processes would seem logical, but the underlying geopolitical tensions that gave birth to them may prove difficult to overcome and an impediment to further CBM elaboration. Of the two, the Open-Ended Working Group with its inclusive membership and a mandate that incorporates ‘development’ as well as ‘study’ would seem the better vehicle for transferring the CBM-related recommendations of successive GGEs into an actual negotiated agreement that states would be committed to. It is noteworthy that even those consultants long

associated with the GGE process have expressed concern that its utility might have expired and that another forum for carrying the work forward should be considered. As James Lewis has noted: 'Over time, the GGE process has evolved into a proxy for negotiations between States, and there have been suggestions that it might be time to move these discussions to a more regular diplomatic process' (UNIDIR, 2016).

It remains to be seen whether the emergence at the UN of a more inclusive and transparent process for multilateral deliberation and negotiation will be able to achieve real progress towards the goal of codifying CBMs relevant to international cyber security in a manner conducive for state agreement and adoption.

Back to the source: the OSCE and cyber CBMs

Given its role during the Cold War as the crucible for developing CBMs for international security, it is appropriate that outside the UN the OSCE remains the regional organization that has made the most progress in developing agreements on CBMs for international cyber security. The 57-member OSCE began to turn its attention to the potential of CBMs for cyberspace in 2011 and by April of 2012 had decided to elaborate a set of CBMs 'to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs' (OSCE 2012 and 2013). The preparatory work progressed rapidly and by the end of 2013 the OSCE Ministerial Council adopted its initial agreement on CBMs.

The set of 11 measures, all except the last cast as voluntary steps, included several promoting information exchange on a wide spectrum of cyber security-related themes as well as those specifying consultations 'in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of ICTs, and to protect critical national and international ICT infrastructures including their integrity' (OSCE, 2013).

The language used by the OSCE in explaining the aims of the CBMs is a clear echo of the terminology employed regarding the existing CBMs in the conventional arms control realm.

Despite the voluntary caveat, there is a certain presumption of action in the OSCE formulations, such as the CBM on consultations cited above and which reflects the consultative practice OSCE states were already familiar with under the Vienna and other security documents.

Significantly, the final measure, #11, is expressed as an operational requirement and is an early example of cyber CBMs being provided with dedicated institutional support. The measure reads:

Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039 to discuss information exchange and explore development of CBMs.

(p. 2)

This allowance for regular follow-up on the CBMs adopted by a dedicated working group represented the type of monitoring that had not been previously attached to CBM proposals and which again was a feature of the OSCE's handling of its conventional military CBMs. Also important was specifying the use of OSCE platforms, including the OSCE Communications Network run by the Secretariat's Conflict Prevention Centre, for the exchange

of information indicated in the CBM package, which aligned it with existing practice for conventional military CBMs.

The institutional impetus provided by the Informal Working Group facilitated further development of cyber security CBMs despite the deterioration in overall East–West relations. In March 2016 a further five CBMs were adopted by the OSCE. States were encouraged ‘to investigate the spectrum of co-operative measures as well as other processes and mechanisms that could enable participating states to reduce the risk of conflict stemming from the use of ICTs’ (OSCE 2016). It was further specified that the information exchange envisaged in the CBMs would occur on an annual basis and ‘in a manner that maximizes transparency and utility’.

There is little public information available as to how well the agreed CBMs are being implemented and the nature of the Informal Working Group’s on-going work to promote them. An infographic from 2016 suggests that the percentage of member states having implemented at least one of the 16 CBMs has increased from 61% in 2015 to 90% in 2016 (OSCE, 2018b). This of course provides little basis for judging the extent of implementation and the quality of the exchanges amongst member states regarding the CBMs. Still there is no question that the OSCE has gone the farthest of any regional organization in agreeing on CBMs and providing institutional support for their operationalization. As the current chair of the Informal Working Group, Ambassador Karoly Dan of Hungary has stated without an excess of modesty: ‘The OSCE is a shining example for organizations like the ASEAN Regional Forum and the Organization of American States who are facing the same cyber/ ICT security challenges and threats’ (OSCE, 2018a).

Conclusion: future directions for CBMs

In considering both the CBMs articulated by the UN GGEs (most notably in the 2015 report) and the 16 adopted by the OSCE since 2016, there are clear commonalities of concern. In keeping with the overall conflict prevention rationale, and the support that transparency and predictability provide in this regard, CBMs that establish communication channels, promote information exchange and protect critical infrastructure emerge as priorities. The OSCE set are generally couched in more operational language than those of the UN and while the ‘on a voluntary basis’ condition is widespread there is a presumption that activity will occur.

The presence in the OSCE of an on-going dedicated body, the Informal Working Group, as a nexus for CBM development, and crucially for discussion of implementation, is a major distinguishing feature. This institutional support, and the legacy of the OSCE’s decades long experience with CBMs in the conventional military field, does suggest that cyber security CBMs are most likely to gain the greatest adherence among the OSCE member states in the near term. The additional fact that the OSCE comprises 57 states of broadly similar capacity, whereas the UN has 193 member states with wide disparities in cyber capabilities, is of course another advantage the OSCE enjoys.

Neither the UN nor the OSCE is immune however from the detrimental effects of the revival of what has been called ‘great power rivalry’ and the decline in trust amongst leading cyber powers. Work on advancing CBMs however should not be derailed due to a back-drop of geopolitical tensions. It should also not be left only to the biggest cyber powers to set the pace. As the authors of a recent comparative study of UN and OSCE confidence-building have observed: ‘The mistrust between the larger state players – China, Russia and the United States – creates both an opportunity and a need for Middle Powers such as Germany, the Netherlands, Switzerland, Australia, and Canada to demonstrate creative

leadership' (Hitchins & Gallagher, 2018, p. 13). It will be interesting to see the degree to which countries such as these step up to exercise leadership in promoting cooperative measures for conflict prevention. The expansion of the number of states acquiring offensive cyber capabilities and the magnitude of potential damage to states large and small from unrestricted cyber warfare, may serve to press states to become more active in considering diplomatic options for preserving a peaceful cyberspace. In this effort, CBMs from 'tried and true' to more innovative variants are sure to feature prominently.

References

- Grigsby, A. (2018) The end of cyber norms. *Survival*. 59(6) (December-January).
- Hitchins, T. & Gallagher, N.W. (2018) *Building Confidence in the Cybersphere: A Path to Multilateral Progress*. Center for International Security Studies, University of Maryland (March).
- Organization for Security and Cooperation in Europe (OSCE) (1975) *Helsinki Final Act*. Available from: www.osce.org/helsinki-final-act [accessed 13 June 2019].
- Organization for Security and Cooperation in Europe (OSCE) (1981) *Vienna Document 2011 on Confidence and Security Building Measures*. Available from: www.osce.org/fsc/86597 [accessed 13 June 2019].
- Organization for Security and Cooperation in Europe (OSCE) (2011) *Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*. Permanent Council Decision No 1039 (26 April). Available from: www.osce.org/pc/90169 [accessed 13 June 2019].
- Organization for Security and Cooperation in Europe (OSCE) (2013) *Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the use of Information and Communication Technologies*. Permanent Council Decision No 1106 (3 December). Available from: www.osce.org/pc/109168 [accessed 13 June 2019].
- Organization for Security and Cooperation in Europe (OSCE) (2016) *OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*. Permanent Council Decision No 1202 (10 March). Available from: www.osce.org/pc/227281 [accessed 13 June 2019].
- Organization for Security and Cooperation in Europe (OSCE) (2018a) Press release on OSCE Cyber Security Conference in Rome. (28 September) Available from: www.osce.org/chairmanship/397853 [accessed 13 June 2019].
- Organization for Security and Cooperation in Europe (OSCE) (2018b) Infographic on OSCE Cyber/ ICT Security. Available from: www.osce.org/secretariat/390830 [accessed 13 June 2019].
- Tikk, E. & Kerttunen, M. (2018) *Parabasis. Cyber-diplomacy in Stalemate*. Norwegian Institute of International Affairs. Report no. 5 Available from: <https://nupi.brage.unit.no/nupi-xmlui/handle/11250/2569401> [accessed 13 June 2019].
- United Nations General Assembly (UNGA) (1981) *UN Group of Governmental Experts on Confidence-Building Measures*. A/36/474 (6 October).
- United Nations General Assembly (UNGA) (1999) *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/53/70 (4 January).
- United Nations General Assembly (UNGA) (2004UK) *Developments in the Field of Information and Telecommunications in the Context of International Security – Report of the Secretary General*. Views of the United Kingdom. A/59/116 (23 June).
- United Nations General Assembly (UNGA) (2004US) *Developments in the Field of Information and Telecommunications in the Context of International Security – Report of the Secretary General*. Views of the United States of America. A/59/116/Add.1 (28 December).
- United Nations General Assembly (UNGA) (2005BR) *Developments in the Field of Information and Telecommunications in the Context of International Security – Report of the Secretary General*. Views of Brazil. A/60/95/Add.1 (21 September).
- United Nations General Assembly (UNGA) (2005a) *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/60/202 (5 August).
- United Nations General Assembly (UNGA) (2005b) *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/60/45 (8 December).

- United Nations General Assembly (UNGA) (2011) A/RES/66/24 (2 December).
- United Nations General Assembly (UNGA) (2010) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/65/201 (30 July).
- United Nations General Assembly (UNGA) (2013) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/68/98 (24 June).
- United Nations General Assembly (UNGA) (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174 (22 July).
- United Nations General Assembly (UNGA) (2018) *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/73/27 (11 December).
- United Nations General Assembly (UNGA) (2019) *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/RES/73/266 (2 January).
- United Nations Institute for Disarmament Research (UNIDIR) (1999) *Developments in the Field of Information and Telecommunications in the Context of International Security*. Summary report of private discussion meeting, UN DDA and UNIDIR, Geneva, 25–26 August, 1999. Available from: www.unidir.org [accessed 13 June 2019].
- United Nations Institute for Disarmament Research (UNIDIR) (2007) *ICTs and International Security, Disarmament Forum*. (September) Available from: www.unidir.org [accessed 13 June 2019].
- United Nations Institute for Disarmament Research (UNIDIR) (2016) *Report of the International Security Cyber Issues Workshop Series*. UNIDIR and CSIS (Lewis, J. ed.) Available from: www.unidir.org [accessed 13 June 2019].
- United Nations Office for Disarmament Affairs (UNODA) (2015) *Developments in the Field of Information and Telecommunications in the Context of International Security*. Fact Sheet. Available from: www.un.org/disarmament [accessed 13 June 2019].

EXPORT CONTROLS

The Wassenaar experience and its lessons for international regulation of cyber tools

Elaine Korzak

Introduction

Israeli company NSO Group is currently facing a number of lawsuits from journalists and activists alleging that their products were used to illegally access private communications (Kirkpatrick & Ahmed, 2018). The company – a commercial provider of surveillance technology to government entities worldwide – has frequently made news headlines in past years. In 2016, it was reported that technology sold by NSO Group was used in attempts to access the phone of Ahmed Mansoor, an activist in the United Arab Emirates (Perlroth, 2016). The case was widely covered as the tools used to target his device utilized (extremely rare) zero-day vulnerabilities in the iPhone operating system, prompting Apple to issue a software update (Menn, 2016). Most recently, Citizen Lab at the University of Toronto has tracked the use of NSO software to entities in 45 countries, including those with poor human rights records such as Bahrain, Kazakhstan, Mexico, Morocco, Saudi Arabia, and the United Arab Emirates (Marczak et al., 2018).

The case of NSO highlights an issue that has become an enduring cybersecurity concern: the use and potential misuse of surveillance and intrusion tools, often referred to as ‘spyware’. These technologies are routinely used by law enforcement and intelligence agencies in the pursuit of their legitimate activities. However, following the fall of government regimes during the Arab Spring, numerous cases emerged in which technology was used by repressive regimes in violation of human rights. Devices of human rights activists, political dissidents, opposition leaders and journalists were tracked, accessed and monitored, eventually even leading to arrests and acts of torture.

In response to these revelations, member states of the Wassenaar Arrangement, a multilateral export control regime for conventional weapons and dual-use items, decided to place certain cyber tools that have been associated with human rights violations under export controls. More specifically, in 2013 IP surveillance systems and items related to intrusion software were placed on the Arrangement’s dual-use control list. As a consequence, companies developing and selling these types of tools would have to apply for a license from their government to be able to export their products abroad. With this, the developments in the Wassenaar Arrangement represented a first tangible effort at the regulation of specific

cyber tools through a multilateral instrument. They have even been characterized as a first attempt to regulate ‘digital weapons’ (Moussouris, 2015).

At the same time, the Wassenaar changes have proceeded in relative isolation from broader international efforts to regulate cyber tools that have thus far not yielded concrete results. Throughout the years, calls for ‘cyber arms control’ agreements or ‘cyber weapons’ treaties have been repeatedly made, without tangible outcomes or granularity in discussions. Yet, the experience of the Wassenaar regulations has not been situated in this broader context.

The following chapter seeks to fill this gap and examines the developments in the Wassenaar Arrangement in order to identify valuable lessons for broader international regulatory efforts.

To that end, the first part of the chapter presents and analyses the Wassenaar experience with regard to cyber tools. It introduces the human rights context in which the regulation of cyber tools came about and explains the resulting focus on surveillance and intrusion tools. The items added to export controls in 2013 are described in detail along with their subsequent amendments in 2016 and 2017. These changes became necessary after the national implementation of the 2013 additions failed in the United States. While the Wassenaar additions represent the first international effort to regulate cyber tools, they have also proven to be controversial. The US implementation process was extremely contentious and challenging. A broad coalition of stakeholders, led by cybersecurity industry and research representatives, criticized the proposed guidelines for being too broad, covering a range of legitimate tools used in cybersecurity and defense activities.

Following the in-depth examination of the Wassenaar experience and its controversial nature, the second part of the chapter situates these developments in the broader efforts of the international community to regulate cyber tools. It describes the contours of discussions in the United Nations and contrasts them with the particulars of the Wassenaar experience to argue that the regulation of surveillance and cyber tools represents a discrete and limited regulatory effort. The Wassenaar additions target a specific and limited set of cyber tools that were adopted in a particular political context of enduring human rights concerns surrounding the transfer and use of these tools. Nonetheless, even in light of its discrete character, the Wassenaar experience, and in particular the controversy surrounding US implementation, offers valuable insights for any future initiatives seeking to regulate cyber tools. The remainder of the second part discusses three key lessons: 1) the emergence of new stakeholders and equities, 2) the need to ensure involvement of key states, and 3) the need to address definitional challenges. The last part of the chapter offers concluding thoughts.

Applying export controls to cyber tools: The Wassenaar experience

(Enduring) human rights context

The Arab uprisings of 2011 played a key role in exposing the use of cyber tools by authoritarian and repressive regimes. A number of high-profile cases investigated by major news outlets and human rights organizations illustrated the role of surveillance and intrusion tools provided by predominantly Western companies in the widespread perpetration of human right violations. Gamma International’s FinFisher products were reportedly used by the government of Bahrain to track pro-democracy activists (Privacy International, 2014). In 2015, a breach of Italian company Hacking Team provided insight into sales of cyber tools to countries across the globe, including Azerbaijan, Egypt, Ethiopia, Kazakhstan, Saudi Arabia, and Sudan (Greenberg, 2015).

As a report of the Electronic Frontier Foundation put it,

[t]he reach of these technologies is astonishingly broad: governments can listen in on cell phone calls, use voice recognition to scan mobile networks, use facial recognition to scan photographs online and offline, read emails and text messages, track a citizen's every movement using GPS and can even change email contents while en route to a recipient.

(Cohn, Timm & York, 2012, p. 2)

Unsurprisingly, in light of their capabilities these types of tools have become sought-after technologies by government entities worldwide. McKune and Deibert (2017) argue that overall hacking has become an increasingly utilized technique for law enforcement and intelligence agencies. Legitimate use cases need to be acknowledged: '[i]n some cases it is a necessary component of critical investigations that bear on public security. With standardized end-to-end encryption of consumer communications platforms becoming more prevalent, law enforcement and intelligence agencies are targeting endpoint devices' (p. 3).

However, as the Arab Spring and its aftermath have shown, these technologies also have the potential to be greatly misused by bad faith actors as

not all government utilize due process in authorizing digital attacks. Not all governments target individuals for reasons permissible under international human rights law. Indeed, government misuse of spyware and other advanced dual-use technologies has become a regular and foreseeable occurrence.

(ibid.)

With this, detrimental human rights effects have focused civil society advocacy on the regulation of surveillance and intrusion tools. In 2014, several non-governmental organizations formed the Coalition Against Unlawful Surveillance Exports (CAUSE) calling on governments to regulate '[t]he unchecked development, sale and export' of technologies (Järvinen, 2014).

Multilateral export control mechanisms, in this case the Wassenaar Arrangement, presented an obvious starting point for regulatory efforts. In 2013, the United Kingdom and France proposed a set of additions to the Wassenaar control list on dual-use items that emerged in the described context of human rights concerns and corresponding civil society campaigns. The following section introduces the Wassenaar Arrangement and its scope before describing the cyber additions in detail and the ensuing controversy in their implementation.

The Wassenaar Arrangement

An integral part of the international nonproliferation regime, the 'Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies' was established in 1996 (Wassenaar Arrangement, 2017a). Its goal is to promote 'transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations' (ibid., p. 4). It focuses on transfers of conventional arms and dual-use items which are to be regulated through a harmonization of national export control policies. As such, Wassenaar does not ban the transfer of conventional weapons or dual-use items. Rather, an inclusion of items under the Wassenaar Arrangement means that participating states commit to control the export of such items through their national export licensing processes involving government review, and approval or denial (Pyetranker, 2015).

Items can be placed on one of two lists maintained by the Arrangement: the ‘Munitions List’ covering conventional weaponry and the ‘List of Dual-Use Goods and Technologies’ for items that can have both civil and military applications (Wassenaar Arrangement, 2017a). The control lists are updated regularly and decisions to include or exclude an item have to be taken by consensus by the participating states (*ibid.*). Wassenaar’s membership includes a diverse set of countries beyond the major industrial countries, including the US and European states, as well as Russia, South Africa, and most recently India (Wassenaar Arrangement, 2017b; Wassenaar Arrangement, 2018). Notable states not participating are China and Israel.

Lastly, once additions are made to Wassenaar’s control lists, changes have to be implemented at the national level vesting participating states with a great deal of discretion. As the founding documents state, ‘[t]he decision to transfer or deny transfer of any item will be the sole responsibility of each Participating States’ (Wassenaar Arrangement, 2017a, p. 5). Thus, the effectiveness of decisions reached in the framework of the Wassenaar Arrangement is critically dependent on the implementation by its participating states.

Cyber additions to the Arrangement

At the initiative of the United Kingdom and France, the plenary meeting of 2013 adopted a set of controls to cover certain surveillance and intrusion tools (Privacy International, 2015). The addition of cyber tools was described by the Arrangement as a measure to control technology that ‘under certain conditions, may be detrimental to international and regional security and stability’ (Wassenaar Arrangement, 2017c, p. 47). With these changes, cybersecurity concerns entered export control discussions and have subsequently attracted considerable attention as well as controversy. Broadly speaking, the additions focused ‘primarily on software that facilitates data mining and analysis’ (Pyetranker, 2015, p. 164).

More specifically, the participating states of the Wassenaar Arrangement added provisions concerning two items to be controlled by the List of Dual-Use Goods and Technologies: IP network surveillance systems and items related to intrusion software.

The first item – IP network surveillance systems – was added to the part of the Dual-Use List covering ‘Telecommunications’. Category 5.A.1.j. added IP network systems that could perform certain functions on a ‘carrier class IP network’ such as a national grade IP backbone (Wassenaar Arrangement, 2016, p. 80). These functions include analysis of the application layer, extraction of metadata and application content as well as indexing of extracted data (*ibid.*). In addition, the IP network system communications surveillance system needs to be ‘specially designed’ to carry out a number of processes, including the execution of searches based on hard selectors and the mapping of relational networks of individuals or groups (*ibid.*). If all of these conditions are met, an IP network surveillance system falls under the list of items controlled by the Wassenaar Arrangement.

The second addition to provisions in 2013 covered items related to intrusion software that were made in the ‘Computers’ section of the Dual-Use List. Category 4.A.5. was added to control items that are ‘specially designed or modified for the generation, operation or delivery of, or communication with, ‘intrusion software’ (*ibid.*, p. 72). This provision covers components that are used to generate, install or control intrusion software, rather than intrusion software itself. This differentiation is meant to affect the producers of intrusion tools but not targeted individuals who are likely to have the intrusion software, but not the components used to generate it, on their devices (Bohnenberger, 2017). The provisions related to intrusion software sought to control malware that could be used to surreptitiously establish access to a device to either copy information or execute external commands.

Following the additions of 2013, the provision on IP surveillance systems has remained in place. However, the language concerning items related to intrusion software was subsequently amended in 2016 and 2017. These changes followed the controversial US implementation attempt of the 2013 additions that is described in greater detail below. The US sought to amend the language concerning intrusion software in 2016 and 2017 in order to limit the scope of the provisions. In the end, minor changes were introduced that mainly clarified the scope of existing language and carved out a number of specific exemptions.

In particular, the 2017 meeting of the Wassenaar Arrangement provided a clarification that software updates do not fall under the export control provisions covering ‘intrusion software’ (Wassenaar Arrangement, 2017d). More importantly, the 2017 plenary exempted technology used for ‘vulnerability disclosure’ and ‘cyber incident response’ from the scope of provisions covering items related to intrusion software (*ibid.*). Both exemptions cover routine activities of cybersecurity companies and researchers and directly address concerns that had been voiced during the US implementation efforts.

Whether the provisions covering items related to intrusion software will be further amended or narrowed down in the future is unclear. Similarly, it remains open whether the participating states will seek to include additional cyber tools to be regulated by its export control lists. Thus far, two specific surveillance and intrusion tools were added to the Dual-Use control list in 2013 – IP surveillance systems and items related to intrusion software. The latter has been the subject of continuing discussions and efforts to restrict the scope of controls adopted in 2013.

National implementation and controversy

Following the changes to Wassenaar’s control lists, additions have to be implemented nationally to become effective. The following section describes the implementation and ensuing controversy in key participating states of the Arrangement, namely the United States and EU member states.

Following the changes of 2013, the European Union moved swiftly to add IP surveillance systems and items related to intrusion software to its export control regulations (Bromley, 2017). The prominence of EU-based companies in revelations following the Arab Spring greatly raised awareness among European policymakers. Export controls fall under ‘exclusive’ EU competence, meaning that regulations are legally binding and directly applicable in member states although they are drafted and adopted by European Union organs rather than national parliaments. The current legal basis for the EU’s export controls on dual-use items is Regulation 428/2009 which was adopted in May 2009 (Council Regulation, 2009). Regulation 428/2009 is used to incorporate changes agreed to in multilateral export control mechanisms, including the Wassenaar Arrangement. However, the regulation leaves the implementation and enforcement of export control licensing processes to member states.

These national licensing decisions proved controversial following the incorporation of the Wassenaar additions in the EU. Italy, for instance, reportedly issued global or general licenses that allowed the export of multiple items to multiple destinations over the course of several years (Bromley, 2017). In another instance, Denmark was criticized for authorizing the sale of IP surveillance systems to Qatar (*ibid.*). However, it is difficult to assess the consistency and uniformity of export control implementation in the EU as comprehensive and comparable data regarding national licensing decisions across its member states is lacking.

In addition to the implementation of the 2013 additions to the Wassenaar Arrangement, the regulation of cyber tools has been a part of the official review of the EU dual-use export

control regime that began in 2011. The review seeks to update and ‘recast’ the current framework, chiefly to replace the 2009 Dual-Use Regulation. The Commission has introduced a draft text for a new regulation that needs to be reconciled with the views of the European Parliament and the Council (European Commission, 2016). Agreement has not been reached yet so that the final text of the regulation remains open. However, the draft regulation indicates expanded export controls for surveillance and other cyber tools. Among other things, it places particular emphasis on human rights concerns and defines ‘dual-use items’ broadly to explicitly include ‘cyber-surveillance technology which can be used for the commission of serious violations of human rights or international humanitarian law, or can pose a threat to international security or the essential security interests of the Union and its Member States’ (ibid., p. 19). The proposed changes are not without controversy and it remains to be seen whether the European Union framework will be used to expand controls on cyber tools.

In contrast to the developments in the European Union which incorporated the 2013 additions to the Wassenaar Arrangement, the United States has yet to implement any of the provisions relating to cyber tools. In 2015, the Department of Commerce issued proposed language to include IP surveillance systems and items related to intrusion software in its export control regulations. These changes proved highly controversial. A broad coalition of stakeholders including private industry, cybersecurity researchers and human rights and privacy organizations responded with considerable criticism. Particularly the provisions relating to intrusion software were a source of contention. Opposition to the proposed regulation ultimately led to the decision of the US administration not to go ahead with the implementation process and instead to seek amendments to the original provisions in the Wassenaar Arrangement (Department of Commerce, 2016). These efforts led to the changes of the Wassenaar language in 2016 and 2017 described above that narrowed the scope of provisions related to intrusion software.

Broadly speaking, the controversy surrounding the attempted implementation in the United States was centered on the potential impact of the proposed regulations on cybersecurity activities and research. A broad range of cybersecurity companies and researchers argued that the guidance issued by the Department of Commerce was over-inclusive, covering a number of tools that are commonly used in cyber defence activities and practices (Zetter, 2015). The proposed regulation would not only cover intrusion tools that have been used in connection with human rights violations, but would potentially capture routine activities such as penetration testing, information sharing, or vulnerability disclosure. Such unintended capture would undermine cybersecurity efforts in general.

As outspoken critic Katie Moussouris summarized it,

For human rights advocates, software ... that bypasses security protections, hides from anti-virus and other malware detection tools, and spies on the victim, represent a threat to human life when used by repressive regimes. But for security researchers, the same offense techniques that are developed to bypass existing computer security measures are used in research to highlight weaknesses in order to fix the vulnerable software. These identical techniques simply can't be logically separated from the exploit techniques that are used by criminals and nation states in spyware tools. In other words, these technologies are dual-use – aiding defenders who are testing their security and used by attackers who are up to no good.

(Moussouris, 2015)

In a similar vein, the Internet Association (which includes major technology companies like Amazon, Google and PayPal) asserted that the proposed rules ‘could have a negative impact on our ability to defend our networks from attackers’ (Internet Association, 2015). Export license requirements would negatively impact the ability of industry to perform red team–blue team exercises, and share information within a company as well as with other stakeholders (ibid.). Further, there was particular concern among industry and researchers over the status of research involving vulnerabilities and exploits, which form an integral part of defense and research activities (Moussouris, 2015; Cardozo & Galperin, 2015). Even human rights and privacy organizations shared these cybersecurity concerns (Privacy International, 2015).

The impact of regulations on cybersecurity activities was not the only criticism voiced by industry and civil society stakeholders, but it was the major point of concern. The US administration’s response sought to address some of these core issues with the 2016 and 2017 amendments carving out exemptions for ‘vulnerability disclosure’ and ‘cyber incident response’. Reportedly, industry and research communities have welcomed the recent changes to the Wassenaar Arrangement’s provisions (Waterman, 2017). However, it remains to be seen whether the US will be seeking to further revise the language concerning intrusion software in the Wassenaar Arrangement and whether the US is planning to implement the Wassenaar’s provisions as they currently stand.

The Wassenaar experience in the context of international regulation

International regulation and calls for cyber arms control

The developments within the Wassenaar Arrangement have proceeded in relative isolation from other international efforts aimed at the regulation of cyber tools or capabilities. International cybersecurity discussions have been taking place in the United Nations with complementing and competing activities in various regional forums. These discussions have generally been broader in character, exploring the implications of information and communication technologies (ICTs) for international security and stability rather than focusing on specific tools or capabilities.

The debate within the United Nations was originally initiated by the Russian Federation which has been driving the process with the sponsorship of annual General Assembly resolutions under the title of ‘Developments in the field of information and telecommunications in the context of international security’ (United Nations, 1999a). Discussions have sought to consider existing and potential threats in cyberspace while focusing on the use of ICTs by states and relevant implications for international stability.

Over the past decade, a number of Groups of Governmental Experts (GGEs) have been instituted by the General Assembly that put forward a set of measures to counter potentially destabilizing activities. GGEs in 2009–2010, 2012–2013, and 2014–2015 introduced and developed a set of recommendations to guide the behaviour of states in cyberspace. These recommendations concerned three areas: 1) norms of responsible state behaviour and international law, 2) confidence-building measures, and 3) capacity-building efforts (United Nations, 2010; United Nations, 2013; United Nations, 2015). Taken together, these measures aim to define responsible state behaviour in cyberspace and set standards of expected behaviour. The discussion is framed in terms of norms that outline desirable or non-desirable activities. The GGE of 2014–2015, for instance, proposed 11 voluntary, non-binding norms,

including a norm that states should not conduct ICT activity targeting critical infrastructure (United Nations, 2015).

Within this context, the recommendations concerning norms of responsible state behaviour regulate cyber tools or capabilities only indirectly. The proposed set of norms, rules and principles of state behaviour govern the use of ICTs by states more generally, with reference to different types of activities. Arguably, certain cyber tools or capabilities could be regulated if they are used for, or in connection with, (malicious) ICT activity that is covered by these norms of state behaviour. Other than that, the discussions of the UN General Assembly and the Groups of Governmental Experts make few explicit references to the regulation of specific cyber tools.

However, the UN discussions have been intimately linked with the idea of an international treaty in the area of cybersecurity. Since its beginning in 1998, the Russian initiative has included repeated calls for the negotiation of an international treaty or ‘multilateral legal instrument’ (United States, 1999b, p. 9). At some point, officials suggested that an international treaty could be modeled after existing agreements such as the Chemical Weapons Convention (Markoff & Kramer, 2009).

In addition to Russia’s diplomatic initiatives in the United Nations, calls for an international treaty have also been made by numerous scholars, commentators, and representatives from industry and civil society organizations. Such calls are generally based on the assumption that current regulatory frameworks are either insufficient or incapable of regulating state activities in cyberspace (Mueller, 2014; Wheeler, 2018). Most recently, Microsoft’s Chief Legal Officer has lobbied for the negotiation of a ‘Digital Geneva Convention’ that would commit the ‘world’s governments to implement international rules to protect the civilian use of the internet’ (Smith, 2017). Other calls for an international treaty have been modeled after existing arms control mechanisms for nuclear, chemical and biological weapons laying out different versions of a ‘cyber arms control’ agreement or ‘cyber weapons’ treaty (Geers, 2010; Meyer, 2011). Kilovaty and Mann, for example, argue that a ‘cyber-treaty’ that is based on the Chemical Weapons Convention could ‘require states parties to adopt laws prohibiting private companies and individuals from developing certain offensive codes and techniques’ (Kilovaty & Mann, 2016).

Proposals for an international treaty have, however, been met with significant skepticism by the United States and European states for fear that such a treaty could be used, among other things, to unduly restrict the free flow of information across states (for example, the UK submission in United Nations, 2016). Over two decades of UN discussions an international convention has not materialized, despite repeated diplomatic overtures by Russia. At the same time, the notion of an international treaty has not vanished. As recent as 2017 a Cuban representative openly called for UN negotiations to ‘adopt an international legally binding instrument’ (Rodriguez, 2017).

In the end calls for an international treaty, either from governments or from non-governmental stakeholders, persist. However, overall treaty references tend to be remarkably vague or abstract, providing little guidance on the actual scope of the proposed treaty. It remains unclear whether a proposed treaty would focus on, or include, the regulation of cyber tools. Even proposals for a ‘cyberweapons’ convention modeled after other weapons treaties do not provide much detail on the proposed set of cyber tools or capabilities to be regulated.

Situating the Wassenaar experience

Comparing the experience of the Wassenaar Arrangement with the international efforts described above, it becomes apparent that the regulation of cyber tools through export

controls represents a fairly limited and discrete experience. Ultimately, the Wassenaar experience carries limited potential to be representative of more sweeping international agreements for 'cyber arms control' or 'cyberweapons'. Yet, the additions to the Wassenaar Arrangement have often been characterized as exactly that; namely, a test case or first incarnation of 'cyber arms control'.

The recent developments in the Wassenaar Arrangement are particular and context-specific in a number of ways. First, the Wassenaar Arrangement is by design a multilateral, not universal, export control mechanism limited in its membership and regulatory reach. While it covers the major leading countries in terms of technological innovation and economic growth, several key states are not participating in the Arrangement. More importantly, Wassenaar seeks to regulate only the transfer of conventional weapons and dual-use items. It does not target other aspects in the life cycle of weapons or dual-use items, such as development, possession, or use. Even its regulation of the transfer aspect is limited since it does not institute export bans but is used to manage or control the flow of items across borders.

Second, the additions to the Wassenaar Arrangement were themselves limited. The 2013 changes and their subsequent amendments of 2016 and 2017 covered two items only, namely IP surveillance systems and items related to intrusion software. Participating states did not seek to include broader categories such as offensive cyber tools, cyber weapons, or offensive code and techniques.

Third, this particular set of cyber tools is intimately linked with the specific context in which the changes were adopted. Both amendments were agreed upon following revelations of significant human rights violations across a number of states. Sustained civil society campaigns have highlighted the use and sale of a specific set of systems and malware broadly referred to as spyware or cyber surveillance tools. The changes adopted by the Wassenaar Arrangement cover a subset of these items and can, at least in part, be seen as governments' response to human rights concerns connected with these types of technologies. This stands in contrast to discussions in the United Nations, which have focused on implications of information and communication technologies on international stability without discussing or focusing on concerns over spyware.

Taken together, these aspects render the Wassenaar Arrangement's addition of cyber tools a discrete experience. Yet, despite its human rights context and regulatory limitations, developments within Wassenaar have often been described in the terms used in the international cybersecurity discussions at the UN. In particular, the set of cyber tools added to the Wassenaar Arrangement's control lists has been frequently referred to in offensive or weapon-like language. IP surveillance systems and intrusion software have been labelled as 'sophisticated cyberweapons' (Jones, W., 2013) or 'cyber war technology to be controlled in [the] same way as arms' (Jones, S., 2013).

This tendency has contributed to the risk that the Wassenaar experience and the broader regulatory efforts in the United Nations get conflated. Due in part to definitional imprecision, the Wassenaar regulation of specific cyber tools that were associated with human rights violations has been taken as an attempt to regulate the broader category of cyber tools or capabilities in general. There is a risk that the Wassenaar experience is at times incorrectly understood as an attempt to regulate 'cyber weapons' more broadly.

Such a misperception maybe perhaps not be surprising since the Wassenaar additions represent the first tangible effort at the regulation of specific cyber tools thus far. As described above, international conversations have not resulted in the creation of a dedicated international regime. Thus, by comparison, the additions to the Wassenaar Arrangement

represent a concrete attempt to regulate cyber tools that – even with its limitations – has gained notoriety beyond export controls.

Lessons from the Wassenaar experience

Despite the specific context and limitations of the additions to Wassenaar, the export control experience can provide valuable insights for broader efforts to regulate cyber tools internationally. The Wassenaar additions represent a tangible and concrete effort at regulation. At the same time, as has been described above, these changes have proved to be highly controversial and increasingly polarizing for the different stakeholders engaged in the debate. An analysis of the challenges associated with the Wassenaar additions can yield useful pointers for any future efforts to regulate cyber tools through multilateral mechanisms. The controversy that the Wassenaar changes have engendered can offer a cautionary tale for international efforts as much as it can serve to strengthen future initiatives. To that end, the following points seek to distill three key insights drawn from the challenges in applying export controls to cyber tools.

1) The emergence of new stakeholders and equities

As the Wassenaar additions have illustrated, non-governmental stakeholders, including industry and civil society organizations, play an important, if not critical, role in efforts aimed at the regulation of cyber tools. New equities and stakeholders in a realm that has been traditionally dominated by governments, namely national and international security policy, have emerged.

First, human rights considerations appear to have been instrumental in the adoption of the initial Wassenaar controls in 2013. Advocacy and research organizations have been persistent in calls for the regulation of technology that has been used to perpetrate human rights violations by entities all over the world. Human rights considerations are beginning to emerge as a new equity in the export regulation of dual-use items. Unlike in the area of conventional weapons, where human rights concerns have been considered in the past, these considerations represent a novelty when it comes to export controls of dual-use items (Bromley, 2017).

Second, the controversy surrounding the failed implementation of the Wassenaar additions in the United States has powerfully demonstrated the (potentially limiting) role that private industry can play. The criticism brought forward by private sector companies, along with the cybersecurity research community, led to a significant reversal in the position of the US government. With this, concerns over the impact of regulations on cybersecurity-related industry activities have become a prominent aspect in the US debate and have to some extent shifted the focus away from human rights considerations. Cyber defensive activities have entered export control considerations as a new equity to be taken into account when assessing unintended consequences of regulation.

All these activities demonstrate the importance of considering non-governmental actors and new equities in any international discussion aiming to regulate cyber tools. Stakeholders, particularly in the US, have fundamentally diverging views with regard to the ability of export controls to effectively regulate cyber tools. The resulting controversy provides important lessons for the creation of international regulatory efforts. The consideration and support of non-governmental stakeholders appears to be critically important, particularly for the successful implementation of controls.

2) The need to ensure involvement of key states

The second insight drawn from the Wassenaar experience is by no accounts a novel or surprising lesson, namely the need to ensure the involvement of key states and the importance of consistent and uniform implementation across an instrument's membership.

Even with the relatively limited size of the Arrangement, implementation efforts have proved to be challenging. The controversy surrounding the attempted US implementation has resulted in an uneven implementation of the controls on cyber tools across Wassenaar's membership. While most countries, including member states of the European Union, have implemented the 2013 additions, the US is yet to realize the changes in its domestic export control regulations. This stands in contrast to the potential direction of EU controls, which may move toward the inclusion of a wider set of cyber tools, beyond those agreed upon in the Wassenaar Arrangement.

The marked differences in the implementation of the Wassenaar provisions have weakened the overall effectiveness of the controls. The US represents a significant, if not critical state, in the area of cybersecurity that lags behind in implementation. Within the EU, concerns over consistency and uniformity in enforcement have weakened perceived effects of regulation. Resulting doubts with regard to the utility of export controls are likely to carry over to future regulatory efforts. Thus, the experience of the Wassenaar controls has illustrated the importance and need to ensure the full participation of key states. These concerns are only amplified in light of the limited membership of Wassenaar which does not include important states in terms of technological capabilities such as China and Israel.

3) The need to address definitional quandaries

At their core, the Wassenaar efforts have been characterized by the controversy surrounding the definitions used in the Arrangement's control lists. Definitional quandaries have become an enduring feature of the debate and illustrate that agreed-upon definitions in the field of cybersecurity are fundamental, yet at the same time exceedingly difficult to arrive at. International efforts to regulate cyber tools or capabilities will inevitably have to grapple with the challenges of drafting a definition that captures the targeted cyber tools without producing unintended consequences.

The criticism levelled at the 2013 additions, particularly from industry and research communities, focused on the language used to define items related to intrusion software. Industry representatives and researchers argued that the Wassenaar provisions compared to its intended scope were over-inclusive, capturing legitimate and necessary cybersecurity practices.

The controversy surrounding the Wassenaar definitions illustrates an inherent challenge in the regulation of cyber tools or capabilities – the difficulty of cleanly separating code used for offensive purposes versus defensive purposes through a workable and clear definition. Wassenaar's definitions of intrusion and surveillance tools were based on technical attributes – i.e. the functionalities or capabilities of software. As Dullien, Iozzo and Tam (2015) point out, this reliance cannot produce effective controls 'for the simple reason that intrusion and surveillance systems are technically indistinguishable from a wide variety of security, system administrative, and analytic tools' (p. 16). Any definition based on technical specifications 'cannot be used to distinguish between malicious and innocuous software, as they are thoroughly common to both' (ibid., p. 6). Wassenaar's provisions and the controversy surrounding them powerfully illustrate the challenges of regulating items that are inherently dual-use.

Yet, the need for precise and clear definitions cannot be overstated. Any international regulation of cyber tools or capabilities will be critically dependent on the ability of actors to define the type of tools that are covered. In the case of export controls and the Wassenaar Arrangement ‘the capacity to define an item with legal precision in a manner that can be employed at some state prior to the transfer’ is essential as ‘categories on the dual-use list are traditionally based on precisely defined performance metrics’ (Bohnenberger, 2017, p. 87). Furthermore, export controls are typically designed for items that have to be physically moved across borders. Cyber tools are challenging in this regard due to their intangible aspects and the relative ease of software transfer. As Pyetranker argued,

cyber technology is based on data and is therefore completely unlike the scores of tangible dual-use products that the Wassenaar Arrangement controls. The latter can be physically inspected at a border. The former comprises knowledge and speech in the form of strings of numbers and letters.

(Pyetranker, 2015, p. 178)

The Wassenaar experience so far has demonstrated the difficulties of drafting precise definitions, even for a specific subset of cyber tools – those that have been associated with human rights concerns. These definitional challenges are not mitigated by the use of the term ‘cyber weapon’. On the contrary, the term has become a popular shorthand for a variety of activities thereby providing little conceptual clarity or precision. The surveillance and intrusion tools regulated by the Wassenaar Arrangement have been no exception in this regard, despite the narrow focus of controls. As others have noted, ‘[c]yberweapon’ has become a catch-all term for diverse forms of malicious software (malware) for which an extraordinary range of capabilities is claimed (Stevens, 2017, p. 2).

Concluding thoughts

International efforts to regulate cyber tools or capabilities face a difficult environment. Discussions in the United Nations have only indirectly addressed the regulation of cyber tools, lacking any granularity with regard to the scope, structure, and operational aspects of a regulatory mechanism. The concept of responsible state behaviour seeking to set standards for the use of information and communication technology by states has been at the forefront of discussions without mitigating pressing concerns regarding the proliferation of cyber tools and capabilities.

In this context, the developments in the Wassenaar Arrangement have attracted considerable attention as they represent a concrete attempt to regulate a specific set of cyber tools. As such, Wassenaar has at times been understood as a test case for the broader regulation of cyber tools. However, the relationship between these efforts has not been explored, a gap in understanding this chapter has sought to address.

To that end, the analysis of the Wassenaar experience was subsequently contrasted with the developments in international cybersecurity policy discussions to illustrate the limited and discrete nature of the export control regulations adopted. Yet, despite its discrete character, the Wassenaar experience can provide valuable lessons for broader international efforts to regulate cyber tools that have thus far not yielded concrete results. Particularly the controversy and resulting polarization surrounding the US implementation of Wassenaar’s intrusion software controls reveals important insights as it has led to a fundamental questioning of the feasibility of Wassenaar’s export controls. In this way, Wassenaar serves as a cautionary tale, highlighting areas to be considered and addressed in any successful future

regulatory efforts. In particular, analysis showed the emergence and important role played by new stakeholders and equities, the need to ensure the commitment of critical states, as well as the inherent difficulties of crafting workable definitions involving cyber tools.

References

- Bohnenberger, F. (2017) The proliferation of cyber-surveillance technologies: challenges and prospects for strengthened export controls. *Strategic Trade Review*. 3(4): 81–102.
- Bromley, M. (2017) *Export Controls, Human Security and Cyber-Surveillance Technology. Examining the Proposed Changes to the EU Dual-use Regulation*, Stockholm International Peace Research Institute. Available from: www.sipri.org/publications/2017/other-publications/export-controls-human-security-and-cyber-surveillance-technology-examining-proposed-changes-eu-dual [accessed 14 May 2019].
- Cardozo, N. & Galperin, E. (2015) What is the U.S. doing about Wassenaar, and why do we need to fight it? *Electronic Frontier Foundation*. Available from: www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation [accessed 14 May 2019].
- Cohn, C., Timm, T., & York, J.C. (2012) *Human Rights and Technology Sales: How Corporations Can Avoid Assisting Repressive Regimes*. Electronic Frontier Foundation. Available from: www.eff.org/document/human-rights-and-technology-sales [accessed 14 May 2019].
- Council Regulation (2009), *Regulation (EC) No 428/2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-Use Items*. Available from: <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32009R0428> [accessed 14 May 2019].
- Department of Commerce (2016) *Letter from Secretary Pritzker to Several Associations on the Implementation of the Wassenaar Arrangement ‘Intrusion software’ and Surveillance Technology Provisions* (1 March). Available from: www.bis.doc.gov/index.php/documents/about-bis/newsroom/1434-letter-from-secretary-pritzker-to-several-associations-on-the-implementation-of-the-wassenaar-arrang/file [accessed 14 May 2019].
- Dullien, T., Iozzo, V., & Tam, M. (2015) *Surveillance, Software, Security, and Export Controls. Reflections and Recommendations for the Wassenaar Arrangement Licensing and Enforcement Officers Meeting*. Draft Report. Available from: <https://tac.bis.doc.gov/index.php/documents/pdfs/299-surveillance-software-security-and-export-controls-mara-tam/file> [accessed 14 May 2019].
- European Commission (2016) *Proposal for a Regulation of the European Parliament and of the Council Setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (recast)*. COM(2016) 616 final (28 September.) Available from: https://eur-lex.europa.eu/resource.html?uri=cellar:1b8f930e-8648-11e6-b076-01aa75ed71a1.0013.02/DOC_1&format=PDF [accessed 14 May 2019].
- Geers, K. (2010) Cyber weapons convention. *Computer Law and Security Review*. 26(5): 547–551.
- Greenberg, A. (2015) Hacking team breach shows a global spying firm run amok. *Wired* (6 July). Available from: www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/ [accessed 14 May 2019].
- Herr, T. & Rosenzweig, P. (2015) Cyber Weapons & export control: Incorporating dual use with the PrEP model. *Journal of National Security Law and Policy*. 8(2): 301–319.
- Internet Association (2015) *Internet Association Comments on BIS Implementation of the Wassenaar Arrangement 2013 Plenary Agreements on Intrusion and Surveillance Items*. Available from: <https://internetassociation.org/072015wassenaar/> [accessed 16 May 2019].
- Järvinen, H. (2014) Human rights orgs form coalition against surveillance exports. *European Digital Rights*. Available from: <https://edri.org/human-rights-orgs-form-coalition-against-surveillance-exports/> [accessed 15 May 2019].
- Jones, S. (2013) Cyber war technology to be controlled in same way as arms. *Financial Times* (4 December). Available from: www.ft.com/content/2903d504-5c18-11e3-931e-00144feabdc0 [accessed 14 May 2019].
- Jones, W. (2013) Treaty limiting weapons exports updated to include cyberweapons. *IEEE Spectrum* (6 December). Available from: <https://spectrum.ieee.org/riskfactor/telecom/security/treaty-limiting-weapons-exports-updated-to-include-cyberweapons> [accessed 14 May 2019].
- Kilovaty, I. & Mann, I. (2016) Towards a cyber-security treaty. *Lawfare* (3 August). Available from: www.justsecurity.org/32268/cyber-security-treaty/ [accessed 14 May 2019].

- Kirkpatrick, D. & Ahmed, A. (2018) Hacking a prince, an emir and a journalist to impress a client. *The New York Times* (31 August). Available from: www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html?module=inline [accessed 14 May 2019].
- Marczak, B. et al. (2018) *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*. Available from: <https://citizenlab.ca/2018/09/hide-and-peek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/> [accessed 14 May 2019].
- Markoff, J. and Kramer, A. (2009) U.S. and Russia differ on a treaty for cyberspace. *The New York Times* (27 June). Available from: www.nytimes.com/2009/06/28/world/28cyber.html [accessed 14 May 2019].
- McKune, S. and Deibert, R. (2017) *Who's Watching Little Brother? A Checklist for Accountability in the Industry Behind Government Hacking*. Available from: <https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab-whos-watching-little-brother.pdf> [accessed 11 May 2019].
- Menn, J. (2016) Apple fixes security flaw after UAE dissident's iPhone targeted. *Reuters* (25 August). Available from: www.reuters.com/article/us-apple-iphone-cyber-idUSKCN1102B1 [accessed 14 May 2019].
- Meyer, P. (2011) Cyber-security through arms control: An approach to international co-operation. *The RUSI Journal*. 156(2): 22–27.
- Moussouris, K. (2015) You need to speak up for internet security. Right now. *Wired* (16 July). Available from: www.wired.com/2015/07/moussouris-wassenaar-open-comment-period/ [accessed 15 May 2019].
- Mueller, B. (2014) Why we need a cyberwar treaty. *The Guardian* (2 June). Available from: www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty [accessed 14 May 2019].
- Perloth, N. (2016) iPhone users urged to update software after security flaws are found. *The New York Times* (25 August). Available from: www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html [accessed 12 May 2019].
- Privacy International (2014) *Bahraini Government, With Help From FinFisher, Tracks Activists Living In The United Kingdom*. Available from: <https://privacyinternational.org/blog/1231/bahraini-government-help-finfisher-tracks-activists-living-united-kingdom> [accessed 13 May 2019].
- Privacy International (2015) *BIS Submission*. Available from: <https://privacyinternational.org/sites/default/files/2018-02/Privacy%20International%20BIS%20submission.pdf> [accessed 14 May 2019].
- Pyetranker, I. (2015) An umbrella in a hurricane: Cyber technology and the December 2013 amendment to the Wassenaar Arrangement. *Northwestern Journal of Technology and Intellectual Property*. 13(2): 153–180.
- Rid, T. & McBurney, P. (2012) Cyber-weapons. *The RUSI Journal*. 157(1): 6–13.
- Rodriguez, M. (2017) *Declaration by Miguel Rodriguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. Available from: www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf [accessed 14 May 2019].
- Smith, B. (2017) *The need for a Digital Geneva Convention*. Speech given at RSA 2017 (14 February). Available from: <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/> [accessed 14 May 2019].
- Stevens, T. (2017) Cyberweapons: An emerging global governance architecture. *Palgrave Communications*. 3, 10 January.
- Stupp, C. (2018) Nine countries unite against EU export controls on surveillance software. *Euractiv*. Available from: www.euractiv.com/section/cybersecurity/news/nine-countries-unite-against-eu-export-controls-on-surveillance-software/ [accessed 14 May 2019].
- United Nations (1999a) *Resolution adopted by the General Assembly, A/RES/53/70*, 4 January.
- United Nations (1999b) *Developments in the Field of Information and Telecommunications in the Context of International Security. Report of the Secretary-General, A/54/213*, 10 August.
- United Nations (2016) *Developments in the Field of Information and Telecommunications in the Context of International Security. Report of the Secretary-General, A/71/172*, 19 July.
- United Nations (2010) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/65/201*, 30 July.
- United Nations (2013) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98*, 24 June.
- United Nations (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174*, 22 July.

- Wassenaar Arrangement (2016) *List of Dual-Use Goods and Technologies and Munitions List*. WA-LIST (15)1 Corr. 1, 4 April. Available from: www.wassenaar.org/app/uploads/2016/04/WA-LIST-15-1-CORR-1-2015-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf [accessed 14 May 2019].
- Wassenaar Arrangement (2017a) *Public Documents Volume I. Founding Documents*, February. Available from: www.wassenaar.org/app/uploads/2015/06/WA-DOC-17-PUB-001-Public-Docs-Vol-I-Founding-Documents.pdf [accessed 14 May 2019].
- Wassenaar Arrangement (2017b) India becomes 42nd WA participating state. *Official Website* (8 December). Available from: www.wassenaar.org/india-becomes-42nd-wa-participating-state-8-dec-2017/ [accessed 14 May 2019].
- Wassenaar Arrangement (2017c) *Public Documents Volume IV. Background Documents and Plenary-related and Other Statements*. Available from: www.wassenaar.org/app/uploads/2017/12/WA_Public_Docs_Vol_IV_Background_Docs_and_Plenary-related_and_other_Statements.pdf [accessed 14 May 2019].
- Wassenaar Arrangement (2017d) *List of Dual-Use Goods and Technologies and Munitions List*. WA-LIST (17)1. Available from: www.wassenaar.org/app/uploads/2018/01/WA-DOC-17-PUB-006-Public-Docs-Vol.II-2017-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf [accessed 14 May 2019].
- Wassenaar Arrangement (2018) About Us. *Official Website*. Available from: www.wassenaar.org/about-us/ [accessed 14 May 2019].
- Waterman, S. (2017) The Wassenaar Arrangement's latest language is making security researchers very happy. *CyberScoop*. Available from: www.cyberscoop.com/wassenaar-arrangement-cybersecurity-katie-moussouris/ [accessed 14 May 2019].
- Wheeler, T. (2018) In cyberwar, there are no rules. *Foreign Policy* (12 September). Available from: <https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/> [accessed 14 May 2019].
- Zetter, K. (2015) Why an arms control pact has security experts up in arms. *Wired* (24 June). Available from: www.wired.com/2015/06/arms-control-pact-security-experts-arms/ [accessed 14 May 2019].

GLOBAL CYBERSECURITY AND THE PRIVATE SECTOR

Anne-Marie Buzatu

Cyberspace: a virtual domain

New interconnected information and communication technologies have equipped governments as well as non-state actors with the tools to conduct worldwide surveillance, influence democratic processes and collect unprecedented amounts of personal and private data. Cyberspace has also impacted the means and methods of warfare and conflict and has been recognized as ‘a new battlefield, coequal with combat on land, sea or air’ (Møller, 2017). Consequently, there now exist new avenues for attack that involve a broad spectrum of actors and upend traditional rules of engagement including the determination of by whom, and even whether, an armed attack has been launched. In response, a growing number of states and private actors have developed sophisticated methods for gathering intelligence and carrying out coercive actions against state and non-state entities.

They have also enlisted the services of private cybersecurity companies to develop both offensive and defensive cyber capabilities as well as intelligence gathering and electronic surveillance. The May 2019 revelation that NSO group, an Israeli company that markets its products to Middle Eastern and Western intelligence agencies, had developed spyware that infects smartphones through a vulnerability in the application WhatsApp sent chills through the user community, especially when it was revealed that this spyware had been found on the phones of human rights activists throughout the world. Incidents such as these raise questions about what kinds of regulations and norms should apply to new technologies and cyberspace, and furthermore who is in a position to effectively oversee and enforce them?

Cyberspace continues to expand, to evolve and to morph at speeds that are difficult for traditional security institutions, such as parliaments, law enforcement agencies and courts, to keep up with and adapt to in effective ways. In numerous cases, the traditional national democratic, state-centric security institutions are structurally ill-equipped to adequately respond to these new security challenges. In the cybersecurity paradigm, good security sector governance requires new thinking, approaches and strategies that support a framework of effective regulation and oversight, the respect for the principle of the rule of law and protection of human rights in order to protect and improve state and human security. However, in order to upgrade good governance in cyberspace accordingly, it is first necessary to

have a better understanding of how cyberspace is constructed, and what actors have effective influence and control.

This chapter aims to look at the specific challenges and opportunities cyberspace raises for the security sector through the lens of the private sector. It begins with a brief explanation of how cyberspace works, highlighting the important role of the private sector in bringing to life and shaping this medium. This is followed by a discussion of some specific challenges to traditional security situations that are particular to the *cybersecurity* sector. Some of the most recent responses to the challenges are then presented, highlighting the important role the private sector has taken to shape and drive these responses. The chapter finishes with a brief discussion about the current state of cybersecurity norms development, identifying emerging norms, and offering some suggestions for their effective implementation. For the purposes of this chapter, the term ‘private sector’ not only refers to commercial actors, but also includes all non-governmental participants in cyberspace including individuals, civil society, non-state armed groups, and other organizations and communities that are organized around identity or political affiliations.

Cyberspace: the nuts and bolts

For all of the wonders and dangers of this online, borderless virtual space, as many have pointed out, cyberspace does have an underlying physical component that is present in, and in most cases under the jurisdictions of, national authorities. For example, a physical server is under the jurisdiction and control of the country within which it is located, and therefore presumably subject to its laws and oversight. However, its connection to and role in sending and receiving information across the wider cyberspace clouds the notions of locality and territoriality. Without going into too much technical detail, it is worthwhile to consider the stuff which makes the Internet possible.

From a technical perspective, cyberspace is housed within physical and wireless pathways, routers, servers and endhosts (PCs, smartphones, IOTs), also commonly referred to as the link layer, through which data, or information, travels. The principal data pathways of this layer are known as the Internet backbone made up of long, undersea mostly privately-owned transnational fibre optic cables that connect core data routers and large, strategically-placed networks. Of note, the whistleblower Edward Snowden revealed in 2013 that the US and UK carried out ‘the largest programme of suspicionless surveillance in human history’ by ‘tapping directly into the Internet backbone’ (Davenport 2015, p. 58).

Data is shepherded through this interconnected labyrinth with assistance from the Internet Protocol (IP), also known as the network layer, and the Transmission Control Protocol (TCP) or transport layer, to help ensure the correct data get to the right destinations. Atop this resides the application layer, or the one users in cyberspace are most familiar with. It is the level from which users surf the web, participate in social media platforms, stream multimedia and save files to the cloud. As such, it is the layer in which a constant stream of new software and programs are being developed and released by mostly private actors, including private commercial companies, independent software and application developers as well as amateur programmers and hackers.

Addresses in cyberspace are managed by the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit corporation founded in 1998 in California, USA. One of the key functions of ICANN is to facilitate the translation of addresses from words [e.g., Facebook.com] to numbers that the network layer can understand, or the Internet Protocol address (IP address), such as 204.15.23.255. For many years, ICANN provided

these services under a contract with the US government. However, in 2016 ICANN cut ties with the US government to provide these services under a multi-stakeholder governance framework.

Technical standards for the hardware and logical layers are developed and maintained mostly by private, non-profit technical organizations composed of information technology experts. Some of the most influential of these include the Internet Engineering Task Force (IETF), a non-profit non-governmental organization comprised of a volunteer network of engineers, operators, vendors and researchers with headquarters in California. Other influential technical standards organizations include the European Telecommunications Standards Institute (ETSI), a technical standards organization with a European focus, as well as the Institute of Electrical and Electronics Engineers (IEEE).

Drawing from the foregoing discussions, a preliminary description of cyberspace would include the following elements:

- An environment in which many activities of daily living analogous to physical life take place, which may impact the human security of its users, but in which such interactions do not require physical proximity of the participants;
- An environment in which many defensive and offensive security activities take place, which may or may not have direct kinetic effects, but which nevertheless have an important influence on national and international security and defence strategies and policies;
- An interlinked, complex technical and transnational environment through which information travels mostly without regard for territorial borders;
- An environment over which there is no centralized body of oversight or control, but over which the private sector has ownership of and control of most of its physical and logical components and for which the private sector develops most of the technical standards.

While the environment of cyberspace does raise important challenges to the traditional state-centric Westphalian approach to oversight, sovereignty and effective control, many of these and similar challenges have already been raised—and to some degree addressed—by multistakeholder governance initiatives in other sectors, such as the private (physical) security and multinational clothing manufacturing industries. By and large these initiatives have taken a more horizontal *human-security approach* to improving governance and oversight, emphasizing protection of civil society's human rights over the top-down enforcement of state obligations (Buzatu, 2015).

International cybersecurity

The term cybersecurity has been used in a variety of contexts, often with very different meanings for various communities, governments, and private companies. On one hand, cybersecurity may connote the security measures for physical computer systems and networks to protect them from unauthorized and/or malicious access. Increasingly, however, the term cybersecurity is also used to refer to protective measures against a much more diverse array of security threats, including threats to human, community, national, and international security. As more and more of our communications, financial transactions, health records, and military exercises take place and are housed online, how we handle and protect these resources can have direct impacts on the traditional security sectors,

such as police, military and judicial, and can give rise to situations of human, national and international insecurity.

As such, what is meant by the term cybersecurity can mean different things to different people, leading to wide-ranging, sometimes parallel discussions that often fail to yield practical results. Against this backdrop, it is worthwhile to try to disaggregate some of these different aspects with a view to better understanding the challenges posed by cybersecurity in order to begin shaping possible responses.

Traditional security challenges digitized

Taking a closer look at how digital space can shape the security sector landscape, we can identify the following twists on traditional security challenges:

- National/international security threats and responsibilities which may include attacks on national and regional defence capabilities, attacks on critical infrastructure and public and common goods, the use of commercial software applications/private contractors in counter-espionage, facilitation of violent extremism/terrorism through new technologies;
- Human security such as protection against discrimination and cyber bullying, protection of personal data and property against intrusion and theft, respect for privacy and freedom of expression, protection from unlawful surveillance.

In addition, while not wholly distinct from the previous two, the following issues highlight specific challenges relevant to the cyber context:

- Security of technical and logical infrastructure of cyberspace including all of the physical hardware and software components that allow information to flow across cyberspace, to be stored and secured;
- Security of public functions and democratic processes which could include weakening the effectiveness of national institutions, policies and regulation, as well as 'stealing,' unduly influencing or undermining the credibility of democratic elections, referenda and other expressions of popular will;
- Security of private sector data and information systems which would include the information and integrity of both commercial and non-governmental organization information system installations and networks.

To put these challenges into a more relatable context, let us consider a hypothetical example.

Cybersecurity: a hypothetical scenario

Lycian authorities have obtained messages and postings by suspected members of a Lycian-designated terrorist group the authorities they say violate Lycian law on the US-headquartered social media platform Facebook. This group is also suspected of planning a terrorist attack on Lycian soil. Suspects are Lycian nationals residing in Germany and US nationals living in the US. Based on a warrant from Lycian courts, Lycia provides requests for information to Facebook to provide 1) all messages and information posted by the suspects on their platforms, 2) all traffic data (e.g., time stamps, location information) for the identified subjects. Because of the time-sensitivity of the situation, Lycia insists there is not enough

time to go through the traditional Mutual Legal Assistance processes where their requests are reviewed by national authorities, and instead requests that the company immediately releases the information directly to them.

To analyse this hypothetical properly would far exceed the scope and purpose of this chapter. Nevertheless, considering the hypothetical along the lines of the challenges listed above, the following issues come to the fore:

Human security:

- Rights to privacy, protection of data and freedom of expression of the alleged suspects.
- Conflict of laws: which countries' laws and standards for free speech and privacy apply to the online statements – US First Amendment, GDPR, Lycian law?
- Rights to physical integrity and security of those in Lycia who could be hurt by such an attack.

National/regional security threats and responsibilities:

- National security threats Lycia faces with a possible terrorist attack in the planning.
- Potential security responsibilities relevant to the US regarding persons/citizens residing on its territory against a potentially hostile foreign power

Security of technical and logical infrastructure of cyberspace:

- Security of the information systems housing the allegedly illegal messages obtained by Lycian authorities
- Identification of appropriate norms and standards to govern how national intelligence agencies proceed in obtaining data and information from cyberspace?

Security of private sector data and information systems:

- Beyond the individual human security concerns, the confidence and trust of users that their privacy and data will be protected on the company's platform within the computer systems.

Security of national regulation, democratic processes and common goods:

- The weakening/bypassing of US and German legal protections for their residents by Lycia directly requesting Facebook to provide Lycian governmental officials information on alleged suspects residing outside Lycia based on a warrant issued by Lycian courts.

On this last point, consider Facebook's April 2018 Terms of Service (TOS), which say that Facebook can respond to legal requests when it has 'a good-faith belief that a response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards.' Applying that standard to the hypothetical described above, the first two conditions would seem to be met *de facto*, while the condition 'consistent with internationally-recognized standards' would require a determination by Facebook of 1) the correct 'internationally-recognized standards' that apply to this request, and 2) the manner in which to apply them.

As the above discussion demonstrates, the role of the private sector in affecting and even substituting for the State's role and authority to implement international law and standards in cybersecurity is both significant, and in many cases largely dependent on companies' terms of service that have not been developed through democratic or public processes. Despite the

democratic governance concerns it raises, this outsourcing of public oversight functions to private companies is part of a growing trend of governments relying on companies to make important decisions about how to protect human and potentially national security concerns. In fact, in 2018 both the US and the EU adopted new legislation (US: 'the Cloud Act'; the EU: e-evidence) that allows law enforcement authorities to get electronic evidence directly from companies located in other jurisdictions, relying in large part on the companies themselves to make determinations about national and international law and how they apply to the data of individuals (US HR, 2018; EU, 2018).

In parallel, companies have taken initiatives to develop cybersecurity principles and standards, sometimes partnering with civil society organizations and governments, as will be discussed further below.

Private sector responses to cybersecurity threats

As has been previously discussed, the private sector plays an influential role in shaping how cyberspace evolves and develops, including technical and even legal norms and standards. Drawing on their technical understandings of how cyberspace functions, including its most important weaknesses, some of the largest ICT companies have banded together to develop principles and norms that aim to improve security in cyberspace. In terms of ICT company initiatives, Siemens *Charter of Trust* and the Microsoft *Tech Accord* are currently the most prominent. Additionally, some governments have partnered with companies to launch similar initiatives of their own, including France's *Paris Call to Action* to improve trust and security on the Internet, and France and New Zealand's *Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online*, which seeks to curtail terrorist acts and violent extremism.

Siemens Charter of Trust

In February 2018 Siemens, along with eight other ICT companies, launched the *Siemens Charter of Trust* (the Charter) with the objective to support improved cybersecurity. The Charter sets out three primary objectives: to 1) Protect the data of individuals and companies, 2) Prevent damage to people, companies and infrastructures, and 3) Create a reliable foundation on which confidence in a networked, digital world can take root and grow. They further identify ten key principles which they seek to operationalize along their supply chain. (Siemens 2018)

As of the time of this writing, another eight companies announced their support for the Charter, bringing the total to 16. Not all of these companies are traditional ICT companies. For example, Airbus, the European aircraft maker, Total, the French petroleum company, and Allianz, the German insurance and financial services company among others, have joined the ranks of more traditional ICT companies such as IBM, Dell and Cisco Systems. Conspicuously missing from this group are the so-called 'Big 5 Tech companies' Facebook, Amazon, Apple, Microsoft and Google (FAAMG), however the absence of these companies' participation can be explained in part when considering the logic of Siemens' approach: using its leverage as the top dog of a long supply-chain to impose standards down the line in order to reduce cybersecurity weaknesses that can occur at all stages of manufacturing and production.

In February 2019 Siemens went a step further along this path by adopting binding cybersecurity requirements for all of companies within its supply chain, saying that starting from

15 February 2019 Siemens would be introducing these requirements progressively into their existing contracts, and that they would be included in a 'separate, binding clause in all new contracts.' Siemens describes the requirements as those that require suppliers to implement 'special standards, processes and methods into their products and services' with a view to preventing cyberattacks. (Siemens 2019)

As such, Siemens is making implementation of these standards binding as a matter of contract law, a legal regime of obligations that is less complicated by extraterritoriality than is national law. While innovative, this approach is not wholly novel, as imposing cyber risk mitigation standards down the supply chain has figured in cyber resilience policies developed by both private risk management companies and governments (e.g., UK Green Paper 2019). Furthermore, similar approaches translating international standards into contractual obligations have been used in multi-stakeholder initiatives in other sectors, i.e., the Fair Labor Association (FLA) in the clothing manufacturing sector and the International Code of Conduct for Private Security Service Providers Association (ICoCA) in the private security sector. As such, Siemens can use the power of contractual obligations to incentivize their business partners to comply with cybersecurity standards, and has the gamut of contractual remedies including financial damage at their disposal to hold the companies down the supply chain accountable when violations occur.

Microsoft initiatives

The large productivity tech company Microsoft has taken a visible and active role in trying to shape cybersecurity norms through a number of audacious initiatives that seek to influence how cyber war is carried out by States, as well as taking aim at a number of issues important to human security. Some of the most sweeping of these are considered below.

The Digital Geneva Convention

In 2017, Microsoft President Brad Smith wrote a blog on the Microsoft website and spoke at a number of international conferences, including an address to the United Nations at Geneva in November 2017, about 'The need for a Digital Geneva Convention.' Citing the alarming growth of not only cybercrime, but also the proliferation of attacks on nation states, it called on the governments of the world to 'implement international rules to protect the civilian use of the internet.' Using language clearly inspired by the 1949 Geneva Conventions, Smith offered 6 principles to guide such a convention, calling on states to 1) not target tech companies, private sector, or critical infrastructure, 2) assist private sector efforts to detect, contain, respond to, and recover from events, 3) report vulnerabilities to vendors rather than to stockpile, sell or exploit them, 4) exercise restraint in developing cyber weapons and ensure that any developed are limited, precise and reusable, 5) commit to non-proliferation activities for cyberweapons and 6) limit offensive operations to avoid a mass event. (Smith 2017).

The approach was both welcomed as timely and criticized as wrong-headed, with critics saying that a private company – even one as large and influential as Microsoft – was not the right actor to launch an initiative that was destined for states. After several months of seeking the spotlight, the initiative seemed to revert to the background while Microsoft set its sights on other, less contentious avenues.

The Microsoft Tech Accord

In April 2018, Microsoft along with 33 other companies launched the *Microsoft Tech Accord* (Tech Accord), a statement of commitments with a view to reducing threats on the Internet ‘from criminal to geopolitical’ and to ‘improve the security, stability and resilience’ of cyberspace. The Tech Accord sets out 4 commitments of its members:

1) We will protect all of our users and customers everywhere; 2) We will oppose cyber-attacks on innocent citizens and enterprises from anywhere; 3) We will help empower users, customers and developers to strengthen cybersecurity protection; 4) We will partner with each other and with likeminded groups to enhance cybersecurity.

(Microsoft 2018).

This approach got a much more positive reception from the global community, with companies and governments alike applauding the initiative. At the same time, with a fast-growing membership, the Tech Accord has been gaining recognition as an important voice of the technology sector on the international level, issuing several endorsements and statements vis-à-vis ongoing processes. These include both public and private initiatives, such as supporting the Paris Call for Action in November 2018 (see below) and endorsing the ETSI standards for improving IoT security issued in March of 2019.

As of June 2019, the *Tech Accord* had grown to over 100 members of companies from the technology sector, including Facebook (but not the other three of the ‘Big 5’). It also has continued to influence public security discussions on national and international levels. Citing interference in 2016 US and 2017 French elections by hackers trying to sway their outcomes, the Microsoft Digital Crime Unit, or DCU, disrupted and transferred control of six Internet domains created by a group widely associated with the Russian government and known as Strontium, or alternatively Fancy Bear/APT28, thereby ‘successfully execut[ing] a court order’ with a view to reducing interference of the Russian government on the US November 2018 elections (Smith 2018). On the international scale, the *Tech Accord* published a set of recommendations offering confidence building measures for states on ‘[r]educing tensions in cyberspace’ in April 2019. (Microsoft 2019a). The *Tech Accord* continued Microsoft’s efforts to influence governments at the UN level, calling for ‘inclusion of additional voices in international debates on responsible nation state behavior *[sic]* in cyberspace.’ In this paper, the *Tech Accord* asks the 2019 Group of Government Experts (GGE) (sponsored by the United States) and the 2019 Open Ended Working Group (OEWG) (sponsored by Russia) to not work at cross-purposes, and to include meaningful participation from the private sector and civil society. (Microsoft 2019b)

Microsoft Digital Identity

In April 2019, Microsoft published a White Paper on ‘Decentralized Identity,’ a project which aims to give users control of their own identity credentials on the Internet and beyond. Currently, a user’s identity credentials, or their login and password information, is owned by the platform that they are accessing, such as Facebook, or Gmail. Users have as many login credentials as they have accounts. This creates the potential problem that users can lose track of their many different login ids and passwords for the multiple login portals, they may store them in an insecure way, or they may use the same login and password for multiple accounts. Unfortunately, this latter credential strategy creates the further security risk that if their

account is hacked on one platform, such as Facebook, then the security of all their other accounts where they use the same login credentials is also compromised. Microsoft's proposal responds to this security problem by taking the login credentials out of the hands of the different platforms and services and putting them under the direct control of the individual user.

To do this very securely, Microsoft proposes to use blockchain, a technology that has been out for a little more than a decade and which most famously is the technology used by Bitcoin. The user would be able to create, own and control their own online id independently of any organization or government. This user would subsequently have to 'establish trust' for the id (known as a 'decentralized id' by virtue of its using a blockchain), by getting endorsements on its trustworthiness from multiple existing 'trust providers' such as educational institutions, businesses and governments. The more trust provider endorsements a decentralized id gets, the more confidence outside institutions will give it.

Microsoft's initial objective is for all of a user's online accounts to be accessed through one decentralized id, thereby obviating the need for multiple sets of login credentials, and also taking the identifying information out of the hands of the online platform thereby drastically lowering the risk of identity/credential theft. Another objective is to use the substantially-increased security protocols afforded by blockchain as an independent, trusted standard for verifying the authenticity of electronic documents such as those issued by schools and universities, financial institutions and even governments. For example, if a university graduate wanted to have a verified copy of her diploma sent to a prospective employer, this could all be handled electronically almost instantaneously through the block chain verification system, with both the university certain of the identity of the person making the request, and the employer confident of the authenticity of the diploma.

Eventually this could lead to trusted ways to prove one's identity that don't rely on government backing, but rather are vouched for by a combination of other trusted partners, such as schools, banks, and online portals.

This kind of approach would be particularly beneficial for those who have difficulty in obtaining recognized identity documents, such as refugees. As a matter of fact, UNCHR is considering proposals to develop a 'unique digital identity' for refugees in order to combat the difficulties that refugees and others lacking trusted documents encounter in participating in economic, social and political life (O'Neal, 2019).

Government-led multi-stakeholder initiatives in cybersecurity

With cybersecurity concerns rising higher among the priorities of policy agendas, governments are increasingly trying their hand at launching multi-stakeholder initiatives with a view to responding more effectively to cyber threats. Interestingly, many governments are adopting a 'private-sector approach' in these initiatives, using similar language and calls to action. One of these initiatives is the *Paris Call for Trust and Security in Cyberspace*.

Paris Call for Trust and Security in cyberspace

Launched in November 2018 at the Internet Governance Forum (IGF) held in Paris, President Emmanuel Macron joined by over 200 members of governments, civil society and commercial actors called for the international community to support 'Trust and Security in cyberspace' by agreeing to comply with the following principles:

- increase prevention against and resilience to malicious online activity;
- protect the accessibility and integrity of the Internet;

- cooperate in order to prevent interference in electoral processes;
- work together to combat intellectual property violations via the Internet;
- prevent the proliferation of malicious online programmes and techniques;
- improve the security of digital products and services as well as everybody's 'cyber hygiene';
- clamp down on online mercenary activities and offensive action by non-state actors;
- work together to strengthen the relevant international standards.

These principles echo many of those made by private sector initiatives, adopting a style that is more familiar to businessmen and IT professionals than to lawyers and diplomats. Perhaps this helps to explain both the large increase in endorsement, as well as the comparatively strong support for the initiative from the private commercial and civil society sectors. At the time of writing only a few short months after the initiative had been launched, support had more than doubled to 552 endorsements, composed of 66 States, 139 international and civil society organizations, and 347 entities of the private sector. At the same time, superpowers Russia, China and US have not endorsed the Paris Call, bringing into question the strength of the initiative.

Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online

In response to the March 2019 attacks by Australian right-wing extremist on mosques in Christchurch, New Zealand, New Zealand Prime Minister Jacinda Ardern and French President Emmanuel Macron launched the 'Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online.' At the same time, companies Amazon, Facebook, Google, Twitter and Microsoft stepped up to support the Christchurch Call, issuing a joint statement proclaiming that they would take all steps to 'fight the hatred and extremism that lead to terrorist violence.' Furthermore, they issued nine concrete steps – five on the part of the companies alone, and four in collaboration with governments and/or civil society, that the multi-stakeholder participants will take to implement the Christchurch Call.

Concerning the five actions, companies pledged to:

- 1) update their terms of use to 'expressly prohibit the distribution of terrorist and violent extremist content,' 2) establish methods within their platforms for users to report on terrorist and violent extremist content, 3) enhance technology to better detect and remove such content using technologies such as artificial intelligence or digital fingerprinting, 4) implementing measures to make it less likely that livestreaming is used to disseminate such content, and 5) to publish transparency reports on a regular basis regarding 'the detection and removal of terrorist or violent extremist content' including the methodology they used in this process.

In terms of the four 'Collaborative Actions', companies committed to work 'collaboratively across industry, governments, educational institutions, and NGOs': 1) to better understand the contexts of terrorist and violent extremist content in order to develop technology that is more effective in removing offensive content; 2) to develop crisis protocols to respond quickly to terrorist or violent extremist events; 3) to educate the public about how to report or not spread terrorist and violent extremist content online; and 4) companies pledged to

work with NGOS to combat hate and bigotry with a view to working on their underlying causes.

This model is interesting because it is an example of governments launching an initiative and the companies responding to the call for action by providing the substantive content and action points for the initiative. As such, it offers a model of governments taking the lead on a political level, and companies providing both the subject-matter expertise and know-how that it will take to realize the vision. Furthermore, it underscores more broadly the ownership and ability of companies and the private-sector to effectively implement actions in order to combat terrorism and violent extremism.

Cybersecurity norms creation 2.0

The need for global cybersecurity norms that underlie effective regulation and governance of cyberspace is recognized by most stakeholders, including governments, companies and civil society, and only continues to grow as our societies, businesses and individuals increasingly rely on the Internet. Within this interconnected paradigm, a new approach to international norms and standards development in which ICT companies and the civil society sectors are taking on larger, and more influential roles vis-à-vis national governments is taking shape. Perhaps this is precisely because such a configuration of public and private actors collaborating, in many cases side-by-side, most closely resembles the Internet itself: an assortment of different components and actors connected in various ways through their roles, responsibilities and obligations communicating through emerging interoperable norms and standards.

Furthermore, in like fashion to cyberspace, it is often difficult to say where the borders lie that demarcate clear cybersecurity responsibilities: where a government's responsibility ends and a company's begins or where they work concurrently in the same cyberspace, where users of all flavours of expertise contribute to, own, influence and direct the flow and exchange of data. This more free-form, messy configuration necessitates an update to the state-owned top-down approach to norm creation. While state-led diplomatic processes, notably the 2013 and 2015 UN GGE processes, can still contribute to norms creation and evolution, such state-led efforts need to ensure that other important stakeholders such as technical experts, representatives of ICT companies and civil society get more equal floor time.

At the same time, international norms for cybersecurity – even those whose development is led by states – are clearly being influenced by the private sector. Often eschewing the traditional language of diplomats, many state-led initiatives focus more on clear objectives in which the responsibility to implement is shared among those who have the ownership and control to effectively bring them about, regardless of whether they are state or non-state actors. For example, taking a page from the playbook of the International Code of Conduct Association (Buzatu, 2015), one could imagine a scenario where an independent multi-stakeholder organization composed of technical experts, civil society and governments that use human security as the underlying basis for its standards would design the software and security protocols that protect users' human rights. These would be subsequently implemented by governments/companies as regulations or policies with responsibilities for the different stakeholder groups under their jurisdictions/contractual obligations, who would also amend them and keep them up-to-date based on the evaluations and determinations of the independent multi-stakeholder organization. This approach is more concrete than statements such as 'the same human rights apply online that apply offline' because it envisages

clear roles and responsibilities for members of each of the different stakeholder groups in accordance with their own spheres of expertise and areas of 'effective control.' Furthermore, with human security taking centre stage in cyberspace, this would provide an independent, multi-stakeholder feedback loop by which governments'/companies' actions (or inactions) can be measured and offers positive pressures on these entities to respect the human rights of their populations/clients. Under this approach, a paradigm could be said to be emerging where human security is setting the 'gold standard' by which effective cybersecurity governance is measured.

Concretization of norms in a fluid space

In the new paradigm of norms creation, a new overarching norm is emerging from the public-private exchange which reflects the character of cyberspace, namely:

To protect the security, integrity and functionality of data, data systems, software, network architecture and hardware components that 1) contribute to an open, safe and trustworthy cyberspace and 2) that do not cause damage, loss or injury.

From this overarching norm flows a number of more granular norms applying to all relevant stakeholder groups, e.g.,

- Online data, presences and devices of individuals, commercial actors, governments and identity-based communities should not be attacked /integrity should not be violated
- Critical infrastructure and other networked systems important to health, wellbeing and governance processes should not be attacked/integrity should not be violated
- Cyber weapons should be limited, but where they are developed, they should be used for defensive purposes only and must target with precision in a manner that is proportionate to the threat
- Cybersecurity protections should be robust and responsive to new and emerging threats
- Vulnerabilities identified in the cyber ecosystem should be reported and patched as soon as possible
- Procedures to flag and take down online content that incites violence or otherwise attacks users need to be developed and implemented
- Crisis protocols to respond to live incidents of terrorism or violent extremism which instrumentalize cyberspace need to be developed and implemented
- Transparency reports on online content removal and crisis response efforts should be regularly reported
- Education for online users in areas such as what kinds of content should be flagged, as well as what is good 'cyber hygiene' is necessary and should be required in school curricula

The way these norms are formulated does not target a specific stakeholder or assign specific obligations because in most cases implementing these norms will require actions and the responsibility of members of different stakeholder groups working together. Vulnerabilities should be reported by anyone who finds them, regardless of whether they work for the government or an ICT company or are an online user. Cyberweapons should not be launched by any actor except in self-defence. Notwithstanding, these norms still leave many questions

open that would need to be discussed in a multi-stakeholder forum. For example, how do we as an online community define ‘damage, loss or injury?’ How do we approach the pivot point where different national legal systems, each with their own standards for crimes and violations, meet online? Building consensus within the multi-stakeholder community around how to approach these questions, and creating effective mechanisms to practically implement those approaches, will be an important step in the quest to achieve effective governance online.

Oversight and accountability

One area that has been largely absent from these discussions is effective oversight and accountability; instead, there seems to be a tendency within private-sector, multi-stakeholder and even government initiatives to let ICT companies police themselves. This approach is not wholly without merit. Oftentimes existing governance and oversight bodies lack the expertise to determine whether ICT companies are meeting standards or not; at the same time, self-policing lacks independence and credibility. The approach proposed by Siemens to set up a kind of ‘supply-side policing’ chain using the contract as both the carrot and stick has promise, including the possibility that a court of law or arbitration tribunal could review alleged breaches, bringing in independent third-party review. However, even assuming that those bodies do possess sufficient technical expertise to provide effective review and accountability, this begs the question of who is watching and holding accountable Siemens. As a company that has put its reputation very publicly on the line as owner of a secure supply-chain, it has strong incentives to not disclose its own vulnerabilities or breaches. Furthermore, traditional court recourse mechanisms are notoriously slow, and may not be suited to the kind of ‘real-time’ monitoring and oversight that the speed of the Internet often requires.

In response, the author suggests that cybersecurity initiatives take a closer look at some of the multi-stakeholder governance and oversight efforts that have been developed in other initiatives, such as the FLA and ICoCA, as well as the ‘Protect, Respect and Remedy’ framework described in the *UN Guiding Principles for Business and Human Rights* (United Nations 2011). In particular, the author highlights the Global Network Initiative (GNI), a multistakeholder initiative of ICT and communications companies, civil society, academic and other non-state actors (but not states) launched in 2008 in response to the increase in governments making information requests to takedown or block content, restrict access to communications platforms or to hand over user data. GNI developed a set of principles for companies grounded in international human rights standards, and participating companies provide regular reports of government requests and agree to take part in a bi-annual independent assessment of their activities and compliance with the GNI Principles (Buzatu, 2016). These initiatives have formulated comparatively nimble and independent monitoring and oversight mechanisms with meaningful stakeholder representation and participation using human security – *instead of international security* – as the yardstick for measuring success. While some governments may see this approach as infringing upon their traditional remits of sovereignty, the author would urge a different interpretation. One that sees governments’ roles as evolving in step with the course of human progress; where governments, companies and individuals alike can bring their expertise, spheres of influence and control to work together towards a common overarching goal: to co-create a more secure and prosperous world both on and offline.

References

- Buzatu, A-M. (2015) *Towards an International Code of Conduct for Private Security Providers: A View from Inside a Multi-Stakeholder Process*. DCAF SSR Paper 12. Available online at www.files.ethz.ch/isn/195090/DCAF-SSR-12.pdf [accessed 25 June 2019].
- Buzatu, A-M. (2016) *Multistakeholder Approaches to Governance: Opportunities and Challenges*. Horizon Working Paper Series. Geneva, DCAF.
- Chappuis, F. (2015) *Security Sector Reform*. SSR Backgrounder Series. Geneva: DCAF.
- Davenport, T. (2015) 'Submarine cables, cybersecurity and international law: An intersectional analysis.' *Catholic University Journal of Law and Technology*. 24(1). Available from: <http://scholarship.law.edu/jlt/vol24/iss1/4> [accessed 18 May 2019]
- European Commission (2018) E-evidence – Cross-border access to electronic evidence regulation.
- France Diplomatie (2018) Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace. Available from: www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in [accessed 23 May 2019].
- Internet Corporation for Assigned Names and Numbers (2016) *Revised ICANN Bylaws and Restated Articles of Incorporation*. Available from: www.icann.org/en/stewardship-implementation/amending-icann-s-bylaws [accessed 18 May 2019].
- Microsoft (2018) Cybersecurity Tech Accord. Available from: <https://cybertechaccord.org/accord/> [accessed 23 May 2019].
- Microsoft (2019a) Reducing tensions in cyberspace by promoting cooperation, recommendations for confidence building measures. Available from: <https://cybertechaccord.org/uploads/prod/2019/04/finaloaswp.pdf> [accessed 23 May 2019].
- Microsoft (2019b) Call for inclusion of additional voices in international debates on responsible nation state behavior in cyberspace. Available from: <https://cybertechaccord.org/call-for-inclusion-of-multi-stakeholders-in-international-debates-on-responsible-nation-state-behavior-in-cyberspace/> [accessed 23 May 2019].
- Møller, M. (2017) *Current Internet Governance Challenges: What's Next?* UNOG-UNITAR Seminar, Geneva (9 November).
- O'Neal, S. (2019) 'Decentralized identity: How Microsoft (and others) plan to empower users to own and control personal data.' *Cointelgraph*. Available from: <https://cointelegraph.com/news/decentralized-identity-how-microsoft-and-others-plan-to-empower-users-to-own-and-control-personal-data> [accessed 22nd May 2019].
- Siemens AG (2018) Siemens Charter of Trust. Available from: <https://new.siemens.com/global/en/company/topic-areas/digitalization/cybersecurity.html> [accessed 21 May 2019]
- Siemens AG (2019) 'The Charter of Trust takes a major step forward to advance cybersecurity.' Siemens AG Press Release (Munich, 15 February). Available from: [www.siemens.com/press/en/pressrelease/?press=en/pressrelease/2019/corporate/pr2019020158coen.htm&content\[\]=Corp](http://www.siemens.com/press/en/pressrelease/?press=en/pressrelease/2019/corporate/pr2019020158coen.htm&content[]=Corp) [accessed 21 May 2019].
- Smith, B. (2017) 'The need for a Digital Geneva Convention.' Available from: <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/> [accessed 21 May 2019].
- Smith, B. (2018) 'We are taking new steps against broadening threats to democracy.' Weblog. Available from: <https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/> [accessed 22 May 2019].
- UK Green Paper (2019) Cyber resilience – Cyber security and business resilience. Available from: www.itgovernance.co.uk/green-papers/cyber-resilience-cyber-security-and-business-resilience [accessed 25 June 2019].
- United Nations (2011) Guiding principles on business and human rights: implementing the United Nations 'Protect, Respect and Remedy' framework.
- US House of Representatives (US HR) (2018) Clarifying lawful overseas use of Data Act (the Cloud Act). H.R. 4943 (02/06/2018).

PUTTING THE TECHNICAL COMMUNITY BACK INTO CYBER (POLICY)

Pablo Hinojosa, Klée Aiken and Louise Marie Hurel

Introduction

In December 2017, at the UN headquarters in Geneva, a workshop was held as part of the IGF program. The dialogue included members of the community of Computer Emergency Response Teams (CERT), academia, and governmental representatives – some of whom had also participated in a UN Group of Governmental Experts, UNGGE, to develop non-binding norms for responsible behaviour of States in their use of ICTs.

The aim of this workshop was to examine international cooperation practices between CERTs (IGF, 2017). The CERT representatives talked about their pragmatic focus in responding to incidents and their work in solving technical problems to restore connections and communications when these were affected or under threat. They were not comfortable when some academics tried to characterize their international collaboration efforts as science diplomacy (Tanczer, Brass & Carr, 2018).

Any attempt to exemplify collaboration between CERTs in a political or diplomatic context, was answered with discomfort, as if entertaining such perception could undermine the technical viability of their response to cyber incidents. However, CERTs have developed extensive international networks of cooperation and have professionalized themselves – all of which is based in informal and formal relationships of communication, trust and information exchange (see Schmidt, 2014; Bradshaw, 2015; Morgus et al., 2015; Skierka et al., 2015).

As the discussion progressed, one of the norms that was proposed by the 2015 UNGGE report, was brought into the conversation:

States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

(United Nations General Assembly, 2015, p. 8)

CERT representatives made it clear that there had been little discussion about this norm within their community. In fact, most of the technical community had not been made aware of its existence or of any implementation efforts underway.

What happened in 2017 at the IGF workshop in Geneva illustrates how international cybersecurity discussions among States have been somewhat detached from the technical operation of networks. For cybernorms to have any meaningful effect, it seems natural to develop technically feasible solutions to operationalizing these norms. However, the technical community has stayed away, often intentionally, from political processes. Notwithstanding, whilst the panel highlights the intent of this technical security expert community to distance themselves from ‘policy’, recent developments and dialogues between CERTs have started to attend with caution to international cybersecurity norms debate – both nationally (Hoepers, 2018) and internationally (Van Horenbeeck, 2018).

Literature on cybersecurity governance has largely focused on state-centric approaches to security (Arquilla and Ronfeldt, 1993; Dunn Cavelty, 2012; Dunn Cavelty, 2013; Finnemore & Hollis, 2016). While legitimate, we argue that these responses fall short in accounting for other actors within the cybersecurity landscape, that are equally or more important to the security, stability and resilience of networked technical systems. This view offers a myopic understanding of norms development (Mueller et al., 2013; Hurel & Lobato, 2018; Hurel, forthcoming) and fails to recognize the practices that underpin the maintenance, security and well-functioning of networks. Recognising the complexity of activities and interests involved in the process of increased digitization of systems and expansion of networks, recent literature has attempted to account for this realm of activity by focusing on non-state actors such as ‘proxies’, cyber mercenaries (Maurer, 2017), cyber insurance companies, the banking sector, civil society organizations and think tanks. In this ‘turn to non-state actors’, specific attention is required to the role of the technical community, in particular Internet Network Operators and CERTs.

As the discussions at the UN and other multilateral fora intensify and the probability of States reaching meaningful agreements on cybersecurity appears low (Bowcott, 2017), it seems pertinent to reflect on the decision-making processes, and whether they would benefit from including different perspectives, such as the point of view of the technical community. We focus on two important actors within this community, the Network Operators and the CERTs or Incident Response Teams, arguing that inclusion of their points of view in international cybersecurity discussions can help to promote an ‘open, secure, stable, accessible and peaceful’ cyberspace (UNGGE, 2015).

To properly address the question of *how international cybersecurity discussions can benefit from including the view of Network Operators and Computer Security Incident Response Teams (CSIRTs)*, we divide the chapter into three parts: the first one provides a critical assessment of the ‘technical community’ in Internet governance and a nuanced approach that accounts for two specific technical expert communities, the Network Operators and the Incident Response Teams. We argue that both perform key functions in maintaining network operations and cooperating for the security, stability and resilience of the same. This section explores practices that guide both communities and the mechanisms they developed to address security threats. The second will explore how these groups have engaged in the development of international cybersecurity cooperation. Finally, we propose ways to bridge the divide between the policy and technical communities, for a meaningful involvement of the latter in resolving the palpable stalemate in norms development and their effective implementation.

Who is the technical community?

The operation, security, stability and governance of underlying systems, networks and protocols rely heavily on the work of the so-called ‘technical community’ – that is, the engineers and experts that design, configure, interconnect, manage, monitor, and maintain the networks. In the ‘Internet governance’ ecosystem, the ‘technical community’ has often been associated with the management of the Internet’s system of unique identifiers – including ‘protocol parameters’, ‘numbers’ (IP addresses), and ‘domain names’ (registered within the DNS) – commonly referred as Critical Internet Resources (CIR) (Mueller, 2004; DeNardis, 2009). This ‘community’ is also indicative of the organizations which have evolved as the recognized custodians that oversee and manage such critical resources, most notably, the Internet Corporation for Assigned Names and Numbers (ICANN), the Regional Internet Registries (RIRs), the Internet Engineering Task Force (IETF), and their related communities.

This interpretation of the ‘technical community’ has served as a general category, indicating the collective identity among these bodies. It draws on experiences from the development of open standards in bodies such as the IETF and broadcasts specific values such as openness (Benkler, 2006), ‘rough consensus and running code’ (Bradner, 1998; Resnick, 2014), peer-governance (Schmidt, 2013), and decentralization. The international development of the field of Internet Governance, commencing in the 90’s with the institutionalization of the Internet technical organizations – also known as I* (I-Star) organizations – and further promoted in the 2000’s by the World Summit on Information Society (WSIS) and the Internet Governance Forum (IGF), has consolidated the role of this community as a ‘stakeholder group’. In other words, a recognizable community that legitimately engages in the policy, norms, and consensus building processes that underpin the development of global Internet governance (see Doria, 2015).

Admittedly, this account can be criticized as a history of Internet governance told from a primarily US-centric perspective, starting mostly with the development of ARPANET. For example, Bhuiyan (2014), Wasserman (2017) and Hurel and Santoro (2018) have presented different, engaging de-centring, historical accounts. Notwithstanding, critiques highlight that the ‘Internet governance technical community’ has been significantly broadened in the context of the IGF, encompassing other bodies such as the World Wide Web Consortium (W3C), TLD operators, large ISPs, Network Operators, Incident Response Teams, among others (Woolf, 2014).

While the history of this international ‘technical community’ – partly developed with what has been characterized as the early 1990s techno-libertarian view (see Mueller, 2010) – invokes dichotomies such as technical vs. political, technical experts and organizations are deeply entrenched in the politics of the Internet. Be it through governments’ pressures on infrastructure (Kuerbis & Mueller, 2017; Musiani & De Nardis, 2016), content regulation (Zittrain & Palfrey, 2008), network traffic (Wright & Breindl, 2013), control of data (Chander and Lee, 2014) or even the tensions between technical organizations (DeNardis, 2009), there is an inherent challenge (or perhaps illusion) of maintaining such poles apart.

Thus, three key considerations underpin our endeavour of understanding the role of specific ‘technical communities’, in particular, Network Operators and CSIRTs in contributing to international cybersecurity norms discussions:

First, *the technical community cannot be taken as a single and coherent group*. While recognising the importance of the role of the technical community as a stakeholder group in Internet

governance, such an understanding has remained restricted to the management of critical Internet resources (see Levinson & Marzouki, 2015). In addition, this study intentionally focuses on security activities (mitigating threats, responding to incidents, addressing redirection of network traffic) as an exercise of re-centring the analysis of technical expert communities on the practices and values that characterize their engagement at the international level.

In this regard, we approach the understanding of ‘technical community’ as a community of practice, characterized by their shared security expertise, knowledge, activities and communication (Wenger, 1998). Network Operators and CSIRTs function as the “first responders” in identifying, assessing, managing and responding to cyber threats (see Skierka et al., 2015). The former monitors and redirects network traffic to guarantee the security, stability and resilience of the network. The latter is primarily concerned with the monitoring, management and reporting of *threats* (i.e., Distributed Denial-of-Service attacks, malware and botnets) and is formed by a worldwide network of expert communities, which includes but is not restricted to information security practitioners, engineers and computer scientists with both technical skills and knowledge on vulnerabilities and threats.

Second, we argue that there is not only something to be said about *how* this technical community has been impacted by government or private control but, most importantly, *how they actively shape global cybersecurity governance*. By focusing on Network Operators, we are able to analyse a community whose primary objective is not necessarily security, but their activities speak directly to the stability, security, and resilience of networks. In contrast to Network Operators, where security is but one dimension of their work, CSIRTs (and wider incident response community) take security as a starting point to their activities. Nonetheless, as the next sections highlight, both are intrinsically embedded in the operational and policy development of global cybersecurity governance.

Third, *the role of technical expert communities in cybersecurity governance is mutable – and perhaps less easily distinguishable from other stakeholder groups*. As previously mentioned, the technical community changed with the emergence of multi-stakeholder processes in Internet governance. As Levinson and Marzouki contend, they acquired roles that were ‘beyond the technical’ and became deeply involved in policy issues (2015, p. 3). While they make that argument in the context of the shift from the select group of technical experts involved at the ARPANET project in the 1960s to early Internet technical bodies in the 1990s (IETF and ICANN), they also note that this organizational level is still what mostly defines ‘who and what the technical community is’.

Similarly, the evolving threat landscape and pervasiveness of networked systems has also contributed to the development of new organizational structures and bodies of expertise to govern borderless threats. As the following sections highlight, the CSIRT community is one of the results of growing concerns with timeliness and capacity to respond and identify threats (see Healey, 2013; Tanczer, Brass & Carr, 2018). However, changes may also represent a threat to the capacity of the security experts to ‘do their job’ and fully participate in this technical community. That is the case, for example, of recent trends to incorporate national CERTs into the governmental cybersecurity agencies (Morgus et al., 2015) or the impact of privacy legislation like the GDPR on key tools such as the WHOIS database. The landscape of practice (Wenger-Trayner & Wenger-Trayner, 2015) through which these two communities operate is, in this sense, the place of political encounters and intrinsic disputes of power over who gets to define what *is* a threat and *how* it should be responded to.

The Network Operators

By Network Operators we understand a professional group of individuals, mainly technical engineers, responsible for managing the hardware, software, and related infrastructure of a telecommunications network. They design (i.e., architect and configure), operate and maintain networks, as well as attend to matters relating to peering and interconnection, routing, network security, and other operational issues.

Mobile operators, Telcos, Global carriers, Internet Service Providers (ISPs), Data Centers, Hosting/cloud providers, Content Delivery Networks (CDNs), Media companies, Internet Exchange Points (IXPs), Academic networks, Corporate networks, Government networks, Sensor, monitoring and surveillance networks: they all employ Network Operators to run their networks, analyse traffic over them, and identify opportunities for peering.

The main job of Network Operators is to connect their users to other users or content hosted in other networks, ensure there are no congestions on links by balancing traffic across multiple links, and seek peering opportunities to ensure the most efficient and cost-effective routes for traffic to and from their networks. To be able to do so, they constantly monitor their network behaviour, and hence are the first ones to observe any signs of network anomalies.

Network Operators ‘build and maintain’ the Internet, a network of networks, through peering and interconnection. This is how ISPs connect and exchange traffic between their customer and customers from other ISPs. They ultimately inform the ways through which Internet routing happens – that is, the processes ‘by which information packets are guided from their origin to their destination by ‘hopping’ from one network to another’ (Mueller et al., 2013, p. 91).

The way networks (i.e. Autonomous Systems) get to map the geography across networks is through the Border Gateway Protocol (BGP). The BGP was developed as a mechanism for providing interdomain (Butler et al., 2010) routing between different Autonomous Systems (AS) and thus securing the interconnection, stability and exchange of routing information between network providers and customers. This process of learning from each other’s network information is necessary for networks to exchange traffic – in the case of BGP, an IP address space that is used within that network – so that the rest of the Internet ‘knows’ how to send traffic to those addresses.

When two ASs connect to each other, it could be through a commercial relationship where ‘transit’ is agreed, or through ‘peering’. Peering occurs when there is sufficient traffic between networks such that the cost of using upstream providers to connect to other networks can be avoided by exchanging traffic directly.

These ‘peering’ relationships are win-win solutions. This ‘direct traffic exchange’ collaboration means that there is *trust* placed into formal and informal agreements – even when operators are competitors in a commercial environment. Network Operator Groups (NOG) and Peering Forums are examples of events where Network Operators interact and negotiate peering arrangements as well as openly share technical experience and good practice. If there is no commercial relationship, there are no obligations: both networks commit to each other voluntarily to keep the traffic balanced. If traffic is not balanced, then they might switch into a commercial ‘transit’ relationship.

The unparalleled ‘proximity’ of Network Operators to the operation and configuration of networks can contribute to the development and implementations of norms and policies (technical, commercial, governmental or public interest-related). Technically, this proximity produces a particular form of networked governance (see Mueller, Schmidt & Kuerbis, 2013)

where operators monitoring different ASs coordinate actions to connect, identify anomalies or redirect traffic. Thus, bringing us back to the blurred lines and tensions between the operational and political, and the difference between technically informed and uninformed policy implementations.

As cybersecurity risks increase, trust and collaborative relationships between Network Operators are not reducing, but becoming stronger – with more peering agreements, more NOGs being setup, more interconnections, and more routes being announced in BGP (CIDR, 2018). This collaboration is another reason to consider this professional group when developing policies that may have operational impact: if not the active implementers of these policies, they will be the ones to solve the technical gaps between norms and operational reality. Therefore, their views are important to consider in international cybersecurity discussions.

The incident response community

The incident response community is a component of the technical community characterized as having an approach focused on ‘solving problems’. Whether called a CERT (Computer Emergency Response Team), CSIRT (Computer Security Incident Response Team), or any in a number of other variations on the acronym, at their core Incident Response Teams share a common mission to perform, coordinate, and support the response to security incidents within a defined constituency (United States, 2012).

The concept of CERTs can find its roots in 1988 with the release of the Morris Worm. The Morris Worm was one of many early examples of self-replicating, unrestricted software that spread across the Internet. While largely accepted to have been non-malicious and payload-free, with little to no long-term negative impact, the Morris Worm’s ability to infect up to 6,000 machines, or roughly 10% of the Internet at that time, highlighted a fundamental challenge: the clear need for improved coordination in an interdependent environment, balanced by a desire to retain the decentralized characteristics that allowed the Internet to develop as dynamically in size and utility as it had (United States, 1988).

To overcome this duality, a post-mortem review of the Morris Worm incident suggested the establishment of computer security response centres. Founded at the Software Engineering Institute (SEI) at Carnegie Mellon University, the first such formalized body, the Computer Emergency Response Team (CERT, now CERT-CC), was established to perform three main functions (Healey, 2013). Roughly boiled down, these functions can be categorized as incident response, coordination, and information sharing.

The review also recognized the importance of developing working relationships with the wider community of experts and organizations and stated that ‘CERT officials recognize the need to establish credibility and support within the Internet community so that its recommendations will be acted on’ (United States, 1988, p. 25).

In practice, there is significant diversity in the type of services and constituency that any given Incident Response Team services. Various mandates could cover national responsibility or focus on a specific sector, serve a single organization, entity, or a vendor’s product range. There is a wide range of proactive and reactive services that a team can tailor based on the need of their constituency and the capacity and capability of the team itself. Regardless of whether the team discussed is a National CERT, a PSIRT (Product SIRT), or organizational CSIRT, they share a common heritage. A look into the origin of the first Incident Response Team offers insight into the identity by which the community as a whole operates to this day.

These foundational values and the inherent need of trust among the wider security and Internet communities are reflective of similar concepts previously explored within the Network Operator community. This in-built interdependence makes collaboration a cornerstone of technical security efforts, but also has an important dimension in the policy space, where decisions and actions taken, even in a targeted or domestic context, can have a wider flow-on impact across networks and borders.

The technical community and international security

While these communities have an undeniable role on the technical side of the security equation, it is less clear if they also do on the policy dimension of international cybersecurity. Before expanding on the challenges and opportunities of bridging the divide between the technical and policy communities, a look at the way these communities have been engaging with the international cybersecurity policy discussions to-date can help set the context of the discussions.

To understand the ways in which Network Operators and Incident Response Teams can and do engage in international cybersecurity policy discussions, it is prudent to look at the conceptualization of security from their technical perspective. At a high level, the aim of network security can be boiled down to the ‘CIA model’ of confidentiality, integrity, and availability (IETF, 1997). *Confidentiality* involves the prevention of unauthorized use or disclosure of information, *integrity* is the safeguarding of the accuracy and completeness of data, and *availability* suggests that authorized users have reliable and timely access.

For Network Operators, the priority is delivery of access, which requires an approach designed to ‘keep the packets moving’, colloquially referred to as running a ‘fast but dirty’ network (Resnick, 2014). While this working modality may seem to side-line security issues, Network Operators remain a critical component of the security of the Internet as a whole. This can produce a differing perspective and approach, inhabiting a space where security concepts and solutions meet with the pragmatic need to run efficient, stable, and commercially viable networks.

The incident response community, as can be expected, holds security much closer to heart, however there is a clear service component in the role of any CSIRT. At the most basic level, these teams “take action to ensure that the progress of the incident is halted and that the affected systems return to normal operation as soon as possible” (United States, 2012, p. 65). While mandates for CSIRTs can be expansive, including proactive measures such as security auditing and awareness raising, the real-time response component of the work prioritizes minimizing the impact of a security incident, eradicating the threat, and recovery of normal network operations or services (Abdelson et al., 2015). How this is achieved can differ depending on the constituency and mandate of the team, however with a focus on preventing as well as recovering and learning from security incidents, a CSIRT’s approach is pragmatically focused on fixing the problem.

Security, in this regard (for both Network Operators and CSIRTs) are process and time-bound. In other words, it is not an end in itself, rather the result of practices – constant monitoring, establishment of trust-networks, communication within the technical expert community, and cooperation with law enforcement and governments – that enable the state of security. As Bill Woodcock (Atlantic Council, 2012) contends in evaluating the 2007 Estonian attack: ‘Mitigation relationships are reciprocal responsibilities, and when an attack needs to be shut down, it needs to be shut down immediately; there isn’t time for argument’.

Furthermore, a commonality across these perspectives is the framing of security as an important component to the service of the network. The interdependent nature of the Internet leads to a fate sharing situation and when paired with the prioritization of keeping the network running, collaboration and trust are at a premium. This collaborative approach comes both out of necessity and as a developed culture. As a veteran in the community often espouses ‘it’s just the sales people [or policymakers in the case of an international security] who compete, network folks need to talk to each other to make sure the network works’ (Smith, 2018).

Effective implementation of network security measures and timely response to a security incident requires establishing trusted relationships between individual networks and draws on the principle that the security of any single network directly impacts the health of the entire ecosystem. Cooperation across upstream and downstream networks, the network where an incident is propagating, and transit networks, for example, can all play a role in resolving an incident. Given the multidimensional nature of the Internet, necessary partners for response can also extend to vendors, law enforcement agencies and users.

This collaborative approach extends further to include proactive security efforts. Trusted communities of experts and practitioners have developed formal and informal mechanisms for information sharing. This can include sharing of best practices and lessons learned as well as threat intelligence that help to increase situational awareness, assess shared risks, and support preventative measures.

It is important to recognize that in practice plenty of gaps develop. These can manifest from less intentional shortfalls such as a lack of capacity and capability, somewhat more neutral but impactful de-prioritization of security concerns, the tragedy of the digital commons, simple neglect, and even intentional or adjacent malicious intent. While reality is naturally disorganized, collaborative principles remain quite central to the functioning of the Internet and the identity of these communities.

From the Network Operators perspective, with a handful of exceptions, the productive intersection with the policy community is rather limited. Even when expanding the term Network Operators to include both the engineers with hands on the network but also their organizations, beyond direct regulatory and legislative issues at the domestic level, there is often little interest in engaging with international security policy issues despite potential implications for the operations and commercial dimensions of their operations.

Incident Response Teams are starting to feature in international cybersecurity policy discussions. Despite some strong intersections in forum such as APEC TEL and through organizations such as ENISA, in policy discussions incident response teams often feature more as the subject of these discussions rather than active participants. In the face of an increasingly contentious Internet security space, Incident Response Teams have been heralded by policy experts as the poster child of cooperative cybersecurity and the workhorse for building confidence in contentious relationships. The 2015 UNGGE consensus report referred at the beginning of this chapter is an example of this trend, where the policy community champions national CERTs as a fix-all solution to build resilience, to drive international confidence-building measures (CBMs), and as an idealized example of how the security community should function.

An increasing recognition within the technical community of the importance of active engagement (Hoepers, 2018; Van Horenbeeck & Aiken, 2018), not only to react to international security discussions, but proactively collaborate for better policy-making, is a prerequisite to building a more productive relationship between the communities.

Whilst trust is at the core of both the technical and the international policy communities, it expresses itself in contrasting settings. The technical community departs from a notion of pre-existing trust: in the authoritative services of the addressing system and the protocols underpinning the whole functioning of the Internet; in the transmission of packets from network to network; in interconnection and peering agreements; and in cooperating to respond to incidents. So, for the technical community, efforts should be about ‘maintaining’ (i.e., not ‘building’) trust in and on the Internet.

In International Relations, the underlying working assumption is the absence of trust (Waltz, 1979), a Hobbesian perception of the ‘state of nature’ where the international system invariably leads to chaos if not reliant on rules. From this perspective, diplomats work on building trust, through some forms of cooperation and try to enter into international agreements to commit to a set of responsible behaviours. In cyberspace, however, the prospect of respecting such international agreements without pre-existing trust, is tenuous.

While it is important to recognize the different approaches to security and trust between the policy and technical communities, this does not negate the inherent benefits that can be derived from meaningful interaction. After all, even though the technical community does not necessarily talk in terms of ‘international peace and security’, these networks of information sharing, trust, monitoring, and maintenance are fundamental for ensuring the security, stability, and resilience of networks at the national, regional, and global level.

Bridging the divide

Misinformed or partially informed policy making can have an impact on the efficacy of a policy decision. This has become more evident, as governments increasingly view cybersecurity as a national security concern (Rid, 2013). This state-centric approach has led to the re-emergence of concepts such as ‘militarization’ (Deibert, 2003; Dunn Cavelty, 2012) ‘cyberwar’ (see Arquilla, 2012; Rid, 2013; Joque, 2018), ‘cyber offense’ and defence (Lin, 2010) to characterize the language and the tools available for identifying, analysing and labelling threats. In this securitized view (Buzan et al., 1998), governments portray themselves as better positioned to successfully determine *what is the threat and how and when it should be assessed* (Hurel, 2016).

Attempts by governments to implement policies such as content take down, have resulted in intentional or accidental BGP hijacking, with severe technical consequences (Singel et al., 2008). In addition, efforts to intercept traffic for cyberespionage or other purposes have also led to disruptive effects. Prematurely calling for measures such as these can have serious implications for the technical functioning of the Internet and flow on impacts on international relations (Kuerbis, 2019).

In such cases, potential misdiagnosis of the challenge may result in an unbalanced allocation of attention and resources based on perception rather than operational intelligence or a reflexive application of national securitization responses that could escalate the chance of conflict. Without measured technical community input, uninformed action by policymakers can have international security implications.

While there are numerous ways the interaction between the technical and policy communities can be mutually beneficial, when considering international cybersecurity, there are three primary avenues that can be fostered to leverage the value brought by the technical community through: expertise, capacity building, and culture.

The expertise and insight that the technical community can offer to policymakers is important to making well-informed decisions. Network Operators and Incident Response

Teams are positioned to offer an authoritative view on how any given policy decision will or will not impact the functioning of the Internet and the services that rely on it. It is critical that policymakers are aware of how decisions could affect the stability of the Internet and whether policy initiatives are technically feasible. Given the interconnected nature of the Internet it is critical that any follow-on or unintended consequences of a course of action are well understood before implemented as the impact has the potential to propagate across borders.

Beyond direct input of expertise into international security discussions, capacity building provides a clear avenue for the technical community to contribute to as well as engage with the work of policymakers. Successful initiatives to build the technical understanding of the Internet amongst policymakers have had a positive impact on the understanding of the technical realities of the Internet as well as an appreciation of the complexity and dependencies on how the technical community functions, which is then reflected in policy decisions. The most common avenues have been security incident desktop exercises at regional and domestic levels such as the OECD, OAS, ASEAN Regional Forum, and other policymaker workshops spearheaded by the technical community. These initiatives develop a long term understanding of the ecosystem that positively influences the day-to-day work of policymakers and establishes a reciprocal working relationship between those involved.

Finally, the value of cultural diffusion can assist in avoiding misunderstandings and close the gap between the communities. A growing understanding of and appreciation of how the Internet technical community functions, can foremost help policymakers preserve what works, ensuring policy decisions adopt a ‘do no harm’ principle. At a secondary level, habitual exposure to the working modalities of the community can help good practice be adopted in certain aspects of policymaking. Such influences could be seen for example during Internet-related discussions at the 2018 ITU Plenipotentiary Conference, where delegates active in ICANN and RIR processes approached these issues with an increased understanding of the topics, but also notable difference in tenor and advocacy. Whether in a multi-stakeholder setting to policymaking or through the integration of a pragmatic problem-solving approach, this dynamic interaction has mutual and lasting benefits.

A handful of examples of this positive cross-pollination between the technical and policy communities include the Brazilian Internet Steering Committee (CGI.br) with a long track record of constructive collaboration between government and other stakeholders; the 2018 Singapore Cybersecurity Act, which benefited greatly from strong outreach to the private sector and technical communities; more active participation in intergovernmental forums, by CERTs in particular, including the Asia-Pacific Telecommunity (APT) and the Asia Pacific Economic Cooperation (APEC); proactive outreach by the Global Commission on the Stability of Cyberspace (GCSC) and UNIDIR to the technical community to offer input into the development of cyber norms; and efforts such as the Incident Response for Policymakers courses organized by the Forum of Incident Response and Security Teams (FIRST) and the IETF Policymakers Program that not only offer instructive opportunities but also expose policymakers to the different working modalities, reflective of similar bridging efforts through Cooperation Working Groups and Special Interest Groups (SIGs) at RIR events and supporting activities for the ICANN Government Advisory Committee (GAC).

These ongoing activities are signs that not only is the value of this interaction being increasingly recognized, but a call to action to the policymaking community to take advantage of these resources as well as to the technical community to be proactive to engage in these discussions. Such initiatives need to move from examples of novel collaboration into the space of habitual good practice. Governments have a unique position to be an enabler and shape the ecosystem for the Internet to thrive and have a positive impact. But policymakers

are just one of many stakeholders that need to work together, trust each other, to make the best of the Internet. Both the technical and policy communities have a shared interest in establishing an ecosystem that fosters the growth of a secure and stable Internet.

Conclusion

The visibility, sophistication, and scale of cyber-attacks have served as a constant reminder of just how vulnerable and exposed the Internet ecosystem has become (see Joque, 2018). It introduces fundamental questions of coordination, responsibility, assessment and response to threats. As this paper suggests, development of international cybersecurity discussions on norms, practices and responsible behaviour should profit from the experience and knowledge on incident response and network management, recognising that there is a need for continuous cross-pollination between the technical expert security communities, in particular Network Operators and CSIRTs.

To respond to the question of how international cybersecurity discussions gain from the view of these two communities of practice (Wenger 1998) we departed from three premises: that i) the technical community cannot be taken as a single and coherent group, ii) they actively shape global cybersecurity governance; and iii) their role and practices change through time.

We sought to break down the notion of ‘technical community’ to focus on what are the practices and values that characterize what we here address as ‘view’. These include *proximity, peering, trust, confidentiality, integrity, reliability and maintenance* of networks. Most importantly, in engaging with this exercise, we sought to highlight the agency of these two communities through the understanding of their practices, thus meaning that there is something to be said about i) how they communicate and engage in ensuring the security, stability and resilience of networks, ii) their own experiences in engaging with international cooperation and iii) how this view might contribute to the international discussions development.

CSIRTs and Network Operators need to communicate, share, trust and coordinate – all of which are lacking in international discussions, or perhaps progressing quite slowly. The experiences from these communities not only indicate that there is, at least at the operational level, cooperation, but still incipient dialogue between both. This offers an opportunity for further cooperation in such a worrying moment for international norms development.

The policymaking and technical communities approach international security from different perspectives. Each community conceptualizes the challenges and opportunities differently, depart from contrasting assumptions about trust, pursue differing goals, utilize different tools, language, and working methodologies. Nonetheless, international norms and policies have an impact in the development, application, and functioning of technology and, conversely, the technical realities can empower or limit the ability of policies to be implemented or function as intended. While there is value in distinction, if not occasional indifference, like with all things Internet, the interdependencies within the ecosystem necessitate the communities to communicate.

The benefit to be gained by fostering a more open and multidisciplinary approach to cyber policy making goes beyond ideological support for a multi-stakeholder model of Internet governance, but to the more direct fact that well informed policymaking processes, which incorporate technical perspectives more immediate to the day to day operation of networks, lead to better policy outcomes. Moreover, the technical community are the partners that will be needed to act, react to, and implement policy decisions and therefore can offer a unique perspective and frank assessment into the impact of a course of action on wider financial, social, economic, political aspects that surrounds the utilization of the Internet.

References

- Abdelson, H., Anderson, R., Bellovin, S., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Gree, M., Landau, S., Neumann, P., Rivest, R., Schillet, J., Schneier, B., Specter, M., & Weitzner, D. (2015) Keys under doormats: mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*. 1(1): 69–79 Available from: doi: 10.1093/cybsec/tyv009 [accessed 3 December 2018].
- An, J. & Yoo, T. (2017) Birth of epistemic community in internet governance: Focusing on internet technical community in Asia. International Studies Association International Conference 2017. 15–17 June 2017, Hong Kong.
- Arquilla, J. (2012) *Cyberwar is Already Upon Us*. Foreign Policy. Available from: <https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/> [accessed 3 December 2018].
- Arquilla, J. & Ronfeldt, D. (1993) Cyberwar is Coming! *Comparative Strategy*. 12(2): 141–165, Available from: 10.1080/01495939308402915 [accessed 3 December 2018].
- Atlantic Council (2012) *Building a Secure Cyber Future: Attacks on Estonia, Five Years On*. Available from: www.atlanticcouncil.org/?id=10323:building-a-secure-cyber-future-transcript-5-23-12 [accessed 3 December 2018].
- Ballani, H., Francis, P. & Zhang, X. (2007) A study of prefix hijacking and interception in the internet. In *Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications* (SIGCOMM '07). ACM, New York, USA, pp. 265–276. Available from: DOI: <https://doi.org/10.1145/1282380.1282411> [accessed 2 December 2018].
- Benkler, Y. (2006) *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. London, Yale University Press.
- Bhuiyan, A. (2014) *Internet Governance and the Global South*. New York, Palgrave MacMillan.
- Bowcott, O. (2017) Dispute along cold war lines led to collapse of UN cyberwarfare talks. *The Guardian*. Available from: www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges [accessed 29 November 2018].
- Bradner, S. (1998) IETF Working Group Guidelines and Procedures. Available from: <https://tools.ietf.org/html/rfc2418> [accessed 11 November 2019].
- Bradshaw, S. (2015) Combatting cyber threats: CSIRTs and fostering international cooperation on cybersecurity. *Global Commission on Internet Governance*. N.23. Available from: www.cigionline.org/publications/combating-cyber-threats-csirts-and-fostering-international-cooperation-cybersecurity [accessed 3 December 2018].
- Broeders, D. (2015) *The Public Core of the Internet. An International Agenda for Internet Governance*. The Netherlands Scientific Council for Government Policy. WRR Report No. 94.
- Buckridge, C. (2018) *ITU Plenipotentiary 2018: What Just Happened?* RIPE. Available from: <https://labs.ripe.net/Members/chrisb/itu-plenipotentiary-2018-what-just-happened> [accessed 29 November 2018].
- Butler, K., McDaniel, P., Farley, T.R., & Rexford J. (2010) A survey of BGP security issues and solutions. *Proceedings of the IEEE*. 98: 100–122.
- Buzan, B., Waever, O. & Wilde, J. (1998) *Security: A New Framework for Analysis*. Boulder, Lynne Rienner.
- CIDR (2018). CIDR Report for Dec 3 18. CIDR. Available from: www.cidr-report.org/as2.0/ [accessed 3 December 2018].
- Cert, V., Ryan, P., Senges, M., & Whitt, R. (2014) A perspective from the private sector: Ensuring that form follows function. In Drake, W.J. & Price, M. (eds) *Beyond NetMundial: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem*. Philadelphia, Center for Global Communication Studies & Annenberg School for Communication at the University of Pennsylvania, pp. 31–37.
- Chander, A. & Le, U.P. (2014) Breaking the web: Data localization vs. the global internet. *Emory Law Journal*, UC Davis Legal Studies Research Paper No. 378. Available from: <http://dx.doi.org/10.2139/ssrn.2407858> [accessed 3 December 2018].
- Clark, D., Chapin, L., Cerf, V., Branden, R. & Hobby, R. (1991) *RFC 1287: Towards the Future Internet Architecture*. Available from: <https://tools.ietf.org/html/rfc1287> [accessed 30 November 2018].
- Deibert, R.J. (2003) Black code: Censorship, surveillance, and the militarisation of cyberspace. *Millennium: Journal of International Studies*. 32: 501–530. Available from: doi: <https://doi.org/10.1177/03058298030320030801> [accessed 25 November 2018].

- DeNardis, L. (2009) *Protocol politics: The Globalization of Internet Governance* (Information Revolution & Global Politics). Cambridge, MA, MIT Press.
- DeNardis, L. (2015) *Global War for Internet Governance*. New Haven, Yale University Press.
- DeNardis, L. & Musiani, F. (2016) Governance by infrastructure. In Musiani, F., Cogburn, D., DeNardis, L., & Levinson, N. (eds) *The Turn to Infrastructure in Internet Governance*. New York, Palgrave Macmillan, pp. 3–24.
- Doria, A. (2015) *How the Technical Community Frames the Internet and Economic, Social and Cultural Rights*. APC. Available from: www.apc.org/sites/default/files/ESCR%20and%20technical%20community_1.pdf [accessed 1 December 2018].
- Dunn Cavelty, M. (2012) The militarisation of cyber security as a source of global tension (February 1, 2012). In Möckli, D. & Wenger, A. (eds) *Strategic Trends Analysis*, Zurich Center for Security Studies. Available from: <https://ssrn.com/abstract=2007043> [accessed 29 November 2018].
- Dunn Cavelty, M. (2013) From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*. 15(1): 105–122. Available from: <https://doi.org/10.1111/misr.12023> [accessed 3 December 2018].
- Finnemore, M. & Hollis, D.B. (2016) Constructing norms for global cybersecurity. *American Journal of International Law*. Cambridge University Press, 110(3): 425–479. Available from: doi: 10.1017/S0002930000016894 [accessed 3 December 2018].
- Global Commission on the Stability of Cyberspace (GCSC) (2017) *Call to Protect the Public Core of the Internet*. New Delhi, GCSC. Available from: <https://cyberstability.org/research/call-to-protect/> [accessed 3 December 2018].
- Healey, J. (2013) Brief history of US cyber conflict. In Healey, J. (ed.) *A Fierce Domain Conflict in Cyberspace, 1986 to 2012*. Vienna, CCSA.
- Hoepers, C. (2018) ONU, OTAN, ITU, GCSC, GCCS, GFCE, Controle de Armamentos: Como decisões políticas e normas globais podem afetar o trabalho dos CSIRTs, a sua segurança e a da Internet. Presentation 7 Fórum Brasileiro de CSIRTs, 14 September. Available from: www.cert.br/docs/palestras/certbr-forum-csirts2018.pdf [accessed 2 December 2018].
- Hurel, L.M. (forthcoming) Securitização e governança da cibersegurança no Brasil. In Reia, J., Francisco, P.A., Barros, M., & Magrani, E. (eds) *Horizonte Presente: Tecnologia e Sociedade em Debate*. Belo Horizonte, Editora Letramento.
- Hurel, L.M. (2016) *Cybersecurity and Internet Governance: Two Competing Fields?* SSRN. Available from: <https://ssrn.com/abstract=3036855> [accessed 3 December 2018].
- Hurel, L.M. & Lobato, L. (2018) Unpacking cyber norms: Private companies as norm entrepreneurs. *Journal of Cyber Policy*. 3(1): 61–76. Available from: doi: 10.1080/23738871.2018.1467942 [accessed: 30 November 2018].
- Hurel, L.M. & Santoro, M. (2018) Brazil, China and internet governance: Mapping divergence and convergence. *Journal of China and International Relations*, 6(1): 98–115. Available from: doi: <https://doi.org/10.5278/ojs.jcir.v0i0.2267> [accessed 29 November 2018].
- Internet Engineering Task Force (IETF) (1997) RFC 2196. *Site Security Handbook*. Internet Engineering Task Force.
- Internet Governance Forum (2017) *IGF 2017 – Day 3 – Room XI - WS38 International Cooperation between CERTS: WS38 Technical Diplomacy for Cybersecurity*. Available from: www.intgovforum.org/multilingual/content/igf-2017-day-3-room-xi-ws38-international-cooperation-between-certs-ws38-technical-diplomacy [accessed 29 November 2018].
- Joque, J. (2018). *Deconstruction Machines: Writing in the Age of Cyberwar*. Minneapolis, MN, University of Minnesota Press.
- Kuerbis, B. (2018) The folly of treating routing hijacks as a national security problem. *Internet Governance Project*. Available from: www.internetgovernance.org/2018/11/29/the-folly-of-treating-routing-hijacks-as-a-national-security-problem/ [accessed 3 December. 2018].
- Kuerbis, B. & Mueller, M. (2017) Internet routing registries, data governance, and security. *Journal of Cyber Policy*. 2(1): 64–81. Available from: doi: 10.1080/23738871.2017.1295092 [accessed 3 December 2018].
- Levinson, N. & Marzouki, M. (2015) IOs and the technical communities in the internet governance institutional complex: Strategies and perspectives. In *The ECPR 2015 General Conference*, Aug 2015, Montreal, Canada. Available from: <https://hal.archives-ouvertes.fr/hal-01214864/document> [accessed 1 December 2018].
- Maurer, T. (2017) *Cyber Mercenaries. The State, Hackers and Power*. Cambridge, Cambridge University Press.

- Morgus, R., Skierka, I., Hohmann, M., & Maurer, T. (2015) National CSIRTs and their role in computer incident response. *New America*. Available from: www.jstor.org/stable/resrep10504 [accessed 10 October 2018].
- Mueller, M. (2004) *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA, MIT Press.
- Mueller, M., Schmidt, A., & Kuebis, B. (2013) Internet security and networked governance in international relations. *International Studies Review*. 86–104. Available from: doi: 10.1111/misr.12024 [accessed 29 November 2018].
- Musiani, F. & DeNardis, L. (2016) Governance by infrastructure. In Musiani, F., Cogburn, D., DeNardis, L., & Levinson, N. (eds) *The Turn to Infrastructure in Internet Governance*. New York, Palgrave Macmillan, pp. 3–24.
- Resnick, P. (2014) *On Consensus and Humming in the IETF*. Available from: <https://tools.ietf.org/html/rfc7282> [accessed 30 November 2018].
- Rid, T. (2013) *Cyber War Will Not Take Place*. London, Hurst & Company.
- Schmidt, A. (2014) *Secrecy vs. Openness: Internet Security and the Limits of Open Source and Peer Production*. Netherlands, Uitgeverij BOXPress.
- Singel, R., Singel, R., Barrett, B., Matsakis, L., Newman, L., Newman, L., Graff, G., & Rich, W. (2008) Pakistan's accidental YouTube re-routing exposes trust flaw in net. *Wired*. Available from: www.wired.com/2008/02/pakistans-accid/ [accessed 29 November 2018].
- Skierka, I., Maurer, T., Hohmann, M., & Morgus, R. (2015) *CSIRT Basics for Policy-Makers. The History, Types & Culture of Computer Security Incident Response Teams*. Washington, DC: New America, Global Public Policy Institute. Available from: www.gppi.net/fileadmin/user_upload/media/pub/2015/CSIRT_Basics_for_P [accessed 2 December 2018].
- Smith, P. (2018) *IPv6 Infrastructure Workshop*. [Presentation] National Information Technology Park, Ulaanbaatar, Mongolia, 22–24 October.
- Sriram, K., Montgomery, D. McPherson, D., Osterweil, E., & Dickson, B. (2016) RFC 7908 problem definition and classification of BGP route leaks. *IETF*. Available from: <https://tools.ietf.org/html/rfc7908#page-3> [accessed 3 December 2018].
- Tanczer, L., Brass, I. & Carr, M. (2018) CSIRTs and global cybersecurity: How technical experts support science diplomacy. *Global Policy*. 9: 60–66. Available from: <https://onlinelibrary.wiley.com/doi/full/10.1111/1758-5899.12625> [accessed 29 Nov. 2018].
- ten Oever, N. & Moriarty, K. (eds) (2012). *The Tao of IETF. A Novice's Guide to the Internet Engineering Task Force*. *IETF*. Available from: www.ietf.org/about/participate/tao/ [accessed 29 November 2018].
- United Nations General Assembly. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE). (2015) *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174. New York, United Nations.
- United States. General Accounting Office (GAO) (1988) *Computer Security: Virus Highlights Need for Improved Internet Management*. GAO /IMTEC-89-57. Washington DC, United States General Accounting Office.
- United States. National Institute of Standards and Technology (NIST) (2012) *Computer Security Incident Handling Guide*. NIST Special Publication 800–61 Revision 2. Washington DC, US Department of Commerce.
- Van Horenbeeck, M. (2018) *FIRST address to the Global Commission on the Stability of Cyberspace*. FIRST. Available from: www.first.org/blog/20180923-GCSC_address [accessed 3 December 2018].
- Van Horenbeeck, M. & Aiken, K. (2018) An Internet of Governments: How Policymakers Became Interested in 'Cyber'. [Presentation] 30th Annual FIRST Annual Conference, Kuala Lumpur, Malaysia, 26 June.
- Waltz, K.N. (1979) *Theory of International Politics*. Reading, Addison-Wesley Pub. Co.
- Wasserman, H. (2017) African histories of the Internet. *Internet Histories*. 1(1–2): 129–137. Available from: doi: 10.1080/24701475.2017.1308198 [accessed 29 November 2018].
- Weissinger L.B. (2017) Modelling trust and trust-building among IT-security professionals. In Tryfonas, T. (ed.) *Human Aspects of Information Security, Privacy and Trust*. HAS 2017. Lecture Notes in Computer Science, vol. 10292, pp. 557–566, Springer. Available from: https://doi.org/10.1007/978-3-319-58460-7_39 [accessed 2 December 2018].
- Wenger, E. (1998) *Communities of Practice: Learning, Meaning, and Identity*. New York, Cambridge University Press.

- Wenger-Trayner, E. & Wenger-Trayner, B. (2015) Learning in a landscape of practice: a framework. In Wenger-Trayner, E., Fenton-O'Creevy, M., Hutchingson, S., Kubiak, C., & Wenger-Trayner, B. (eds) *Learning in Landscapes of Practice: Boundaries, Identity, and Knowledgeability in Practice-Based Learning*. New York, Routledge, pp. 13–30.
- Woolf, S. (2014) What do terms like multistakeholderism, internet governance and technical community really mean? *ARIN*. Available from: <https://teamarin.net/2014/08/29/terms-like-multistakeholderism-internet-governance-technical-community-really-mean/> [accessed 29 November 2018].
- Wright, J. & Breindl, Y. (2013) Internet filtering trends in liberal democracies: French and German regulatory debates. *Internet Policy Review*. 2(2). Available from: <https://policyreview.info/articles/analysis/internet-filtering-trends-liberal-democracies-french-and-german-regulatory-debates> [accessed 3 December 2018].
- Zittrain, J. & Palfrey, J.G. (2008) Internet filtering: The politics and mechanisms of control. In R.J. Deibert & R. Rohozinski (eds), *Information Revolution and Global Politics: Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA, The MIT Press, pp. 29–56.

29

ECONOMIC CYBERSECURITY LAW

A short primer

*Kathleen Claussen**

Introduction

Regulating the cross-border movement of cyber goods and services is one of the most difficult topics or regulatory questions that governments face. As this volume shows, cybersecurity is not the province of a single set of rules. Rather, cybersecurity and the law governing cyberspace span fields and specializations. Often left to specialist cyber policymakers, regulation of cyber activity is often an exercise that neglects existing canons from diverse fields that may be applicable. In fact, cyber's interdisciplinarity can both complicate legal analysis and enhance it. It can also create more creative and innovative legal strategies for addressing wrongful behaviour related to cyber.

The question of regulation of cyber activity is made more difficult, however, by at least three further areas of contestation among states: varying views on the classification and treatment of cyber artefacts; contrasting domestic legal developments surrounding tools to address cyber activity; and, normative disputes as to what constitutes appropriate cyber behaviour. These questions extend across areas of international and domestic law. Resolving them may be a condition precedent to addressing in a meaningful way cyber issues at the global level; for now, though, states are using existing rules from other areas to try to address cyber-related harms while they develop new rules for those harms.

This chapter is among the several in this volume that seek to bridge the divide among approaches to cyber activities. It undertakes a preliminary exploration and analysis of the treatment of cyber in international economic law. It looks first at international trade and cybersecurity, including domestic trade regimes, before turning to issues in international investment law and cybersecurity. What is covered here is only a snapshot of the landscape. These are fast moving policy discussions and what is discussed here is likely only the tip of the iceberg. Space does not permit a longer exposé. Nevertheless, it is useful to take stock of leading present and past initiatives with an eye to future potential: both technological and legal.

* Associate Professor of Law, University of Miami School of Law. Thanks to Anabel Blanco and Arundathi Venkataraman for research assistance.

Trade and cyber

Like cyber, the reach of what is today considered trade law is and has been growing. As the range of products and services crossing borders has grown, states have sought to regulate more fields in trade agreements. Relevant tariff and non-tariff barriers to free trade influenced by or in reference to cybersecurity include export licenses; import bans and other market access restrictions; cyber sanctions; government procurement restrictions; testing, certification and security standards.

One can separate these tools into different areas: some are domestic tools, including some specific to the United States, some are international. Some may be initiated by companies, whereas some require state action. Some involve unilateral legal determinations and some engage independent adjudication. The menu of tools available depends on the type of incident, the type of harm, the time horizon, and the strength or breadth of the evidence you may have. This Part takes up international tools. It looks at rule-making among governments that may have an impact on the cross-border movement of cyber goods and services. These international rules police how governments may develop their domestic rules for that cross-border movement. In other words, trade rules have a threshold-setting and sometimes harmonizing effect to enable global business. They may also have an impact on the types of activities governments may undertake in cyber, but that is a more experimental area of the law. So far, the world has seen only one economic action (discussed in the following Part) that is intended as a response to alleged offensive malicious cyber activity by another government.

The basic concept behind trade liberalization which has dominated trade law and policy around the world over the last half century is that tariffs and other barriers to trade should be lowered to encourage free trade. International instruments seek to achieve this goal by creating reciprocal commitments to lower barriers among states. The principles of external and internal non-discrimination govern those relationships. Many trade instruments today also include enforcement mechanisms through which states may engage in dispute settlement through third-party adjudication. Where one state successfully shows another has not complied with the terms of an applicable trade agreement, it may have recourse to economic sanctions.

There are few trade instruments that make specific reference to cyber; however, most governments take the position that the rules governing how economies may regulate other goods and services also apply to cyber goods and services. Cyber-specific rules, such as those that deal with encryption, test and certification, security standards, and data storage have been under discussion, however, as the following Sections will show. The unique nature of cyber products arguably makes them more difficult to regulate. For instance, unlike traditional goods, many cyber products are not localized in one place, and their potential to reach across geo-political boundaries will tend to defy traditional regulatory practices. Likewise, some cyber products defy definition and classification under existing trade rules. Thus, many of the peripheral issues that will arise in relation to the cybersecurity of imported goods will likely stem from the unusual nature of these products and services.

This Part first examines free trade agreements (FTAs). These are agreements that have been negotiated between two or more economies, often regional in scope, to afford each participating economy duty-free treatment on a wide range of products and services.

They also regulate legislative and administrative policies undertaken by states – including unwritten administrative policies – by limiting types of measures that states can enact where those measures would be, for example, discriminatory, on foreign goods and services. As of 2019, according to the World Trade Organization (WTO), there are nearly 300 FTAs in force. Many are still under negotiation or nearly entering force. Unlike the WTO agreements that were negotiated in the 1990s, these agreements can take account of modern, recent developments in technology, although they do so with considerable variety. The Part then turns to the WTO framework. In both of the following sections, it is worth noting that apart from FTA digital trade chapters, most trade agreements are silent with respect to cyber-specific provisions. Rather, they govern a) goods, b) services, and c) other state regulatory behaviour with respect to standards and regulations of various kinds. There may be impacts on cyber-trade falling in any of those three categories.

Trade agreements

Generally, FTAs have not kept pace with the complexities of the digital economy, although they are increasingly including additional provisions that make reference to digital trade. Roughly 100 FTAs – engaging both developed and developing economies – have e-commerce or digital trade chapters, although they vary widely in scope and depth. (The *Governance of Big Data in Trade Agreements* project at the World Trade Institute is expected to produce a comprehensive study of these provisions by 2020.)

In the United States, where trade agreements are products of collaboration between the legislative and the executive branches, in 2015, the US Congress enhanced its digital trade policy objectives for US trade negotiations. This legislation directs the US Trade Representative to negotiate agreements that: ‘ensure that governments refrain from implementing trade-related measures that impede digital trade in goods and services, restrict cross-border data flows, or require local storage or processing of data’. For the first time, the 2015 legislation refers to the importance of ‘preventing or eliminating government involvement in the violation of intellectual property rights, including cyber theft and piracy’. As a result of this inclusion, the recent negotiation of the United States–Mexico–Canada Agreement includes highly robust digital trade and intellectual property chapters, which include specific provisions on cyber matters.

In fact, the United States has included an e-commerce (now called ‘digital trade’) chapter in each of its FTAs since it signed an agreement with Singapore in 2003. These chapters recognize e-commerce as an economic driver and the importance of removing trade barriers to e-commerce. Most of the e-commerce chapters contain provisions on nondiscrimination of digital products, prohibition of customs duties, transparency, and cooperation topics such as SMEs, cross-border information flows, and promoting dialogues to develop e-commerce. Some US FTAs also include cooperation on consumer protection, as well as providing for electronic authentication and paperless trading. Each includes also certain exceptions to ensure that each party is able to achieve legitimate public policy objectives, protecting regulatory flexibility.

The US–South Korea FTA (KORUS) contains the most robust digital trade provisions in a US FTA currently in force. In addition to the provisions in prior FTAs, KORUS includes provisions on access and use of the Internet to ensure consumer choice and market competition. Most significantly, the language in the KORUS was the first attempt in a US FTA to explicitly address cross-border information flows by recognizing their importance and discouraging the use of barriers to cross-border data. The financial services chapter of

KORUS also contains a specific, enforceable commitment to allow cross-border data flows ‘for data processing where such processing is required in the institution’s ordinary course of business’.

Other economies have been slower to incorporate digital trade and e-commerce provisions, with the notable exception of the states of South America that have for many years developed such rules in their agreements. The European Union’s position is very much complicated by limitations on its ability to negotiate due to a lack of consensus in the European Commission or among EU Member States on a way forward. Conflict within the Commission over questions of privacy management further inhibits decision-making. Cross-border trade in digital goods and services has been an important, albeit rather divisive, part of the negotiations surrounding the Regional Comprehensive and Economic Partnership (ASEAN, 2018a; ASEAN, 2018b), which brings together 16 states in a major trade liberalization alliance in the Asia-Pacific. To support this work, in August 2018, ASEAN held a Cybersecurity Summit in Singapore, which focused on the challenges that arise when attempting to balance ‘the opportunities afforded by the digital economy ... with the increased sophistication of cyber threats in an increasingly networked world’ (EC-Council: CISO Program, 2018).

Initiatives at the World Trade Organization

Multiple international organizations have undertaken initiatives regarding cyber and digital trade, particularly in the interest of developing shared norms. Due to space constraints, I discuss here only the WTO. The WTO is likely the most significant multilateral or international organization for international economic law. The organization is run by its 164 member governments and administered by a Secretariat (World Trade Organization, 2017a). The WTO’s foundation is a series of negotiated agreements that constitute trade rules for its members. As noted above, the WTO agreements, completed in 1994, did not treat cyber issues specifically, but their rules nevertheless have application to cyber-related policies. For example, since 1998, WTO countries have agreed not to impose customs duties on electronic transmissions covering both goods (such as e-books and music downloads) and services. In recent years, discussions on the best ways to handle the concerns raised by cross-border trade in cyber-related goods and services have gained momentum.

Both the WTO General Agreement on Tariffs and Trade (GATT) and the General Agreement on Trade in Services (GATS) include obligations on nondiscrimination and transparency that cover all sectors. I will focus on the possible applications of the GATS here, although to the extent a traded good may be cyber-related, the same non-discrimination rules apply. In the GATS, some specific ICT-related services are mentioned, but not all. Coverage across members varies and many newer digital products and services did not exist when the agreements were negotiated. Although there has been some discussion about expanding the GATS to be more inclusive of cyber, there are no concrete proposals at this time. Already, however, the GATS has been used as a basis for critique of China’s 2017 wide-ranging cybersecurity law which requires companies to disclose intellectual property to the government and store data locally to be allowed to operate in China (Council for Trade in Services, 2017; World Trade Organization, 2017c). China has taken the position that safeguarding cybersecurity is a legitimate regulatory right for each member and therefore it is acting consistently with its GATS obligations. These types of issues continue to be heavily debated.

On the sidelines of the December 2017 WTO Ministerial, a group of over 70 WTO members, including the United States, agreed to ‘initiate exploratory work together toward

future WTO negotiations on trade related aspects of electronic commerce'. This is a plurilateral effort – meaning it would not apply to all WTO members, only those who opt-in. Members are currently discussing which aspects of digital trade they will address in any negotiations. The United States put forth objectives regarding market access, data flows, fair treatment of digital products, protection of intellectual property and digital security measures, and intermediary liability, among others. The US proposal built on the provisions in its FTAs prohibiting digital customs duties and enabling cross-border data flows. China also put forward a proposal in which it seeks 'to clarify and to improve the application of existing multilateral trading rules' with a focus on facilitating e-commerce. The EU has taken the position that the WTO should focus on consumer protection, non-discrimination and market access online, trade facilitation, and transparency. India's proposal was the narrowest, suggesting that the WTO focus on the original work program. At the time of writing, Members reached consensus only on extending the customs duties moratorium and continuing on the existing workplan.

The WTO Information Technology Agreement (ITA) aims to eliminate tariffs on the goods that power and utilize the Internet, lowering the costs for companies to access technology at all points along the value chain. Originally concluded in 1996, the ITA was expanded during the WTO's Tenth Ministerial Conference in December 2015, entering into force in July 2016. The expanded ITA is a plurilateral agreement among 54 developed and developing WTO members who account for over 90% of global trade in these goods. The expanded ITA eliminates tariffs on 201 additional IT products valued at over US\$1.3 trillion per year. In addition, the WTO Trade Facilitation Agreement includes commitments for streamlining electronic processing of customs documentation.

The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement, in effect since 1995, provides minimum standards of intellectual property protection and enforcement. The TRIPS Agreement does not specifically cover intellectual property protection and enforcement in the digital environment, but it has application to the digital environment. WTO members were required to fully implement TRIPS by 1996, with exceptions for developing country members by 2000 and least-developed-country (LDC) members until 1 July 2021, for full implementation. TRIPS aims to balance rights and obligations between protecting private right holders' interests and securing broader public benefits. Among its provisions, the TRIPS section on copyright and related rights includes specific provisions on computer programs and compilations of data. It requires protections for computer programs – whether in source or object code – as literary works under the WIPO Berne Convention for the Protection of Literary and Artistic Works (Berne Convention). TRIPS also clarifies that databases and other compilations of data or other material, whether in machine readable form or not, are eligible for copyright protection even when the databases include data not under copyright protection. Like the GATS, TRIPS predates the era of ubiquitous Internet access and commercially significant e-commerce. TRIPS includes a provision for WTO members to 'undertake reviews in the light of any relevant new developments which might warrant modification or amendment' of the agreement.

Negotiations on a proposed plurilateral Trade in Services Agreement (TiSA) were launched in April 2013, and are occurring outside of the WTO. The 23 TiSA participants account for about 70% of world trade in services and include the United States, EU, and Australia (European Commission 2017). Some key major emerging markets, including Brazil, China, and India, are not currently parties to the TiSA negotiations. Though the final structure and sectors to be covered in TiSA remain under negotiation, setting common rules for digital trade is a key interest of the United States. The chapter or annex on digital trade or

e-commerce would likely address trade barriers to cross-border data flows, consumer online protection, and interoperability, among other areas, similar to the provisions in the proposed TPP. Two obstacles in the TiSA negotiations, however, have been the EU's reluctance to put forward a proposal on data flows or to commit to including 'new services' (many of which are likely to be digital) under TiSA non-discrimination obligations.

WTO discussions have also been increasing with respect to the regulation of cyber security. The WTO Agreement on Technical Barriers to Trade (TBT) governs technical regulations and standards, including those that would apply to matters such as data storage, telecommunications, regulations on encryption, and privacy laws. Beginning in 2017, WTO members raised concerns as part of TBT discussions about cyber security regulations that apply to information and communication technology (ICT) products and their impact on trade (World Trade Organization, 2017b). Specifically, members extensively debated the impact of cyber security laws on trade in high-technology products. The essence of the discussion was that some members were concerned that newly introduced regulations would negatively impact trade in ICT products by 'potentially discriminating against non-domestic companies and technologies, and possibly leading to unnecessary disclosure of commercially confidential and technical information' whereas members introducing the problematic regulations 'highlighted that cybersecurity rules are needed to address national security issues and to ensure consumer privacy' (World Trade Organization, 2017b). Among the most specific trade concerns being discussed recently by members include contentious Chinese and Vietnamese cybersecurity measures (World Trade Organization, 2018). In fact, much of the new discourse surrounding concern over cybersecurity measures has focused on China, which in recent years has 'crafted a significant body of domestic cybersecurity laws, regulations and standards' (Mirasola, 2018).

Finally, as noted above, a critical component of the WTO is its dispute settlement mechanism (World Trade Organization, undated). All major world powers are active participants in the WTO dispute settlement system and, unlike other international dispute settlement mechanisms, most countries, including states that are active cyber operators, seek to comply with the WTO dispute settlement decisions (World Trade Organization, 2004). Using these tools to address cyber activity or cyber-related policies by governments is not without challenges however. While legislative or administrative cyber-related policies (such as data localization policies or consumer-related regulatory measures) may be addressed through these WTO disciplines consistent with other types of similar policies, it remains to be seen whether governments will use the WTO to address malicious cyber activity carried out by other states (Claussen, 2018). Some commentators have suggested that WTO members have not used the WTO dispute settlement mechanism to address certain cyber harms at least in part because of the 'difficulty of formulating claims' that such measures violate WTO agreements (Fidler, 2013). In particular, WTO members face challenges of evidence collection and achieving the requisite standard of proof. Using a WTO agreement in dispute settlement against another member would be a novel, but likely not impossible, application of the rules.

Transnational economic regulatory tools

Internally, governments regulate the import and export of cyber services and products through at least four trade-related administrative means: export controls, import licenses, government procurement requirements, and technical standards. In this context, cyber products and services are sometimes treated as exceptional (like defence products), whereas in others they are treated like any other goods or services and subject to the same WTO-governed regime, with requirements to avoid discriminatory policies.

With respect to export controls, some governments have begun to take more aggressive measures than in the past with respect to cyber. For example, in 2016, the Bureau of Industry and Security (BIS) in the US Commerce Department made revisions to the Export Administration Regulations to subject more international data transfers, including intra-company transfers, to export licensing requirements. The 2016 rules expand the definition of ‘export’ to include releasing or otherwise transferring decryption keys, network access codes, passwords, software, or other information knowing that such actions would permit the transfer of other technology in clear text or software to a foreign national. Other economies, such as the EU have also regulated intrusion software through export control lists since 2015. Modifications have also been made to export control rules regarding intrusion software in recent years through advances among the members of the Wassenaar Arrangement – a group of countries that meet regularly and agree to control certain technologies. The Arrangement’s 41 members include the United States, most EU members, Russia, Turkey, Argentina and South Africa. The group seeks to establish common controls over transfers of ‘dual-use’ goods – those that have both civilian and military applications – and has taken steps to address software vulnerabilities, though with some limited success.

More recently, some cyber products that were formerly export controlled have normalized as industry has adopted them. For example, encryption devices are now readily traded. The United States had previously classified encryption products as munitions and subjected them to strict export controls. Treatment of cryptographic technology remains mixed: Russia maintained extensive national licensing for cryptographic tech; Korea had a disclosure of source code requirement briefly; India and Vietnam each had proposed laws on the use of foreign cryptographic technology. Governments are also making voluntary guidelines for the private sector with same goals in mind. For example, the US National Institute of Standards and Technology developed in 2014 a widely successful Cybersecurity Framework to be deployed by private companies and organizations for the management of cybersecurity-related risks.

On the government procurement side, some governments have taken steps to limit foreign participation in their cyber infrastructure. Both the United States and Canada, for instance, have introduced measures to limit foreign participation in information technology systems procurements. The plurilateral Government Procurement Agreement is agnostic with respect to digital products, but one may expect to see further developments there as economies try to limit their risk with respect to government and critical infrastructures.

The United States stands out among states as also having undertaken to use other domestic economic tools to address cyber behaviour by foreign states. The next Sections focus on these US actions.

Cyber tariffs

Beginning in 2017, the United States has sought to use Section 301 of the 1974 Trade Act – a US law that permits the president to take action against trading partners that are unfairly burdening US commerce – to address acts, policies, and practices of China in cyberspace and with respect to digital products. The United States has identified four such acts, policies, or practices in an investigation: tools to regulate or intervene in US companies’ operation in China to require or pressure them to transfer intellectual property; acts and policies to deprive companies the ability to set market-based terms in their licensing; unfair acquisition of US companies doing cutting edge technology; and, acts of China in supporting or conducting unauthorized cyber intrusions. In its investigation

report issued in March 2018, the US Trade Representative concluded that China is engaged in such acts, policies, or practices and that they are unreasonable or discriminatory and that burden or restrict US commerce (United States of America Executive Office of the President, 2018). Acting on this conclusion, the Trump Administration took both domestic and international trade policy steps. On the domestic side, the president issued proclamations implementing tariffs on a wide range of products imported into the United States from China. On the international side, the United States filed a case at the WTO against China concerning China's patent law practice, which the United States claims is a violation of the TRIPS Agreement. As of June 2019, tariffs remain in place on a long list of Chinese products and China continues to impose retaliatory tariffs on US goods (Claussen, 2018; Bacchus, 2017).

Cyber sanctions

The United States has also pioneered the use of economic sanctions on individuals and groups for malicious cyber activities. On 1 April 2015, US President Obama invoked the US International Emergency Economic Powers Act (IEEPA), which authorizes the US president to impose economic sanctions to respond to a national emergency (United States of America *International Emergency Economic Powers Act 1977*; Bechky, 2018), to create a sanctions mechanism for cyber activities (United States of America Executive Office of the President, 2015). The 2015 order blocks the transfer of property belonging to individuals engaging in 'significant malicious cyber-enabled activities' (United States of America Executive Office of the President, 2015). It describes activities that are reasonably likely to result in, or have materially contributed to, a significant threat to the 'economic health or financial stability of the United States' (United States of America Executive Office of the President, 2015). Where those activities have the purpose or effect of 'causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain', the US Secretary of the Treasury is empowered to take action to block the transfer of property of responsible individuals from within the United States to outside the United States (United States of America Executive Office of the President, 2015; United States of America Executive Office of the President, 2017). President Donald Trump has continued the program (United States of America The White House, 2018).

The cyber sanctions regime presents multiple challenges both to implementation and in principle. First, to be able to impose sanctions on an individual or group, the US government must be able to attribute the cyber activity to that individual or group. It does so without any judicial review or independent evaluation. The US Secretary of the Treasury has the discretion to rely upon whatever level of confidence he chooses. Second, putting a state-related entity on a sanctions list – like any action against a foreign state – involves many political calculations. Third, limited guidance has been provided concerning the 'malicious cyber-enabled activities'. Such activities could include 'unauthorized access to a computer system, including by remote access; circumventing one or more protection measures, including by bypassing a firewall; or compromising the security of hardware or software in the supply chain' to cause harms including the compromise of critical infrastructure, denial-of-service attacks, or significant loss of sensitive information (e.g., personal financial information or trade secrets). Nevertheless, both the Obama and the Trump administrations have used the cyber sanctions in respect of certain individuals and groups believed to be engaged in malicious cyber activity.

President Obama also imposed additional sanctions on North Korea in early 2015 in response to North Korea's alleged involvement in destructive cyberattacks on Sony Pictures Entertainment in November 2014. In addition, the North Korea Sanctions and Policy Enhancement Act of 2016 codifies sanctions with respect to destructive North Korean cybersecurity activities. The Act defines 'significant activities undermining cybersecurity' to include significant efforts to deny access to or degrade, disrupt, or destroy an information and communications technology system or network or infiltrate information from such system or network; significant destructive malware attacks; and significant denial-of-service activities. The Act also requires the president to impose sanctions on third-country actors who support to certain North Korean activities.

Investment and cyber

Foreign investments are increasingly the focus of government regulation, largely with security interests in mind. Economies such as the United States and Europe have strengthened their foreign investment review systems at the same time that some developing states have opted-out of investment protection regimes. Unlike trade, there is no multilateral investment agreement. This Part takes up, first, the bilateral investment system and, second, regulatory programs that aim to restrict foreign investment. Both have connections with cyber activities although in very different manifestations.

Bilateral investment treaties and investment arbitration

In contrast with trade agreements that seek to open market access for states in reciprocal fashion, bilateral investment treaties (BITs) provide safeguards for investors making investments in foreign countries. They require governments not to discriminate against foreign investments and to provide them fair and equitable treatment, among other obligations. Under the dispute settlement mechanisms of BITs, an investor may sue an infringing state or a state may sue another state party to the treaty.

Nothing in the most recent (2012) US Model BIT (United States of America Department of State, 2013) speaks specifically to cyber harms, although that would not preclude an investor or state from bringing a case alleging harm to an investment through cyber intrusion. To date, there have been no public cases involving cyber harms or focused on cyber policies taken by states; however, cyber issues have arisen in multiple cases including with respect to the consideration of evidence (John, 2016; International Centre for Settlement of Investment Disputes, 2017). This Section describes a handful of these known cases – cases involving typical investments but where cyber hacking led to the creation of evidence. In addition, cyber media have been used to facilitate arbitrations. For example, in some circumstances, blockchain technologies are being applied in conducting arbitrations as well (Shehata, 2018).

A number of investment arbitration tribunals have had to consider whether to admit or to afford any weight to evidence obtained through illicit cyber means. Thus far, no panel as afforded any weight to such documents. For example, while an arbitration between a U.K. company and Turkey was ongoing, in a parallel court-ordered money laundering investigation, the Turkish government intercepted privileged and confidential correspondence and materials that were exchanged between the company and its counsel in connection with the arbitration. These documents were excluded from the arbitration and were ordered to be destroyed (International Centre for Settlement of Investment Disputes, 2008). Similarly, in an arbitration against Kazakhstan (International Centre for Settlement of Investment Disputes,

2017), a US company sought to introduce into evidence documents available on a website after a hack of the Kazakhstan government's computer network. The tribunal ruled that documents protected by legal privilege could not be admitted into evidence, but the other documents could (Ross, 2015 as cited in John, 2016 and Ortiz, 2018).

Documents obtained and made public by Wikileaks have figured in investment cases as well. In an arbitration against Venezuela, a Panamanian company sought to introduce into evidence obtained by Wikileaks (International Centre for Settlement of Investment Disputes, 2011). In its arbitration against Turkmenistan, the Turkish Claimant-company relied upon Wikileaks 'cables' introduced by Turkmenistan (International Centre for Settlement of Investment Disputes, 2013). In a further case, after the decision on merits had been rendered, Venezuela sought a limited hearing for the arbitral tribunal to, inter alia, consider evidence revealed in Wikileaks cables (International Centre for Settlement of Investment Disputes, 2014).

With increasing digitization of all aspects of international arbitration – in filings, seeking and storing evidence and documents in discovery, communications between arbitrators, counsels and parties and arbitral institutions, draft and final awards, and the workings of entire arbitral institutions, for instance – information related to international arbitration is becoming increasingly vulnerable to threats of cyber security breaches. The on-going conversations are either stand-alone scholarship by publicists and practitioners (Cohen & Morril, 2017; Pastore, 2017), or legislative-like endeavours by the Working Group comprising International Council for Commercial Arbitration, the International Institute for Conflict Prevention and Resolution and the New York City Bar Association (International Council for Commercial Arbitration, the International Institute for Conflict Prevention and Resolution & the New York City Bar Association, 2018), the International Bar Association (International Bar Association, 2018), and international law firms (Debevoise & Plimpton, 2017). Each of these publications and endeavours attempts to assign or suggest best practices for each of the different participants (International Council for Commercial Arbitration, the International Institute for Conflict Prevention and Resolution & the New York City Bar Association, 2018) in the arbitral process separately (International Bar Association, 2018; Debevoise & Plimpton, 2017; International Council for Commercial Arbitration, the International Institute for Conflict Prevention and Resolution & the New York City Bar Association, 2018). While a baseline of declarations urging participants of the arbitral process to adopt secure means of conducting an arbitration is a step in the right direction, systemic change will only be seen when there is a standardization of cybersecurity features across the globe and the profession.

Restrictions on foreign investment

Many developed countries have programs that allow them to restrict foreign investment on the basis of national security. For example, the Committee on Foreign Investment in the United States (CFIUS) is charged with reviewing transactions involving foreign participants that could pose a threat to US national security. On this basis, transactions involving technology companies of various types have increasingly come under scrutiny. Some commentators have suggested that this restrictive activity will inhibit the development of new and important technologies, including with relation to cyber.

Likewise, the Trump Administration has increasingly imposed restrictions on ICT providers through emergency powers authorities. In May 2019, the president issued an order declaring that foreign adversaries of the United States were 'increasingly creating

and exploiting vulnerabilities in [ICT] and services ... to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people.... To deal with this threat, additional steps are required'. On this basis, the Administration enabled the US Secretary of Commerce to review and restrict transactions that pose a risk to the security of the United States. On the same basis, the US Commerce Department has also taken steps in 2019 to add more companies, notably the Chinese company Huawei, to its Entities List, meaning that it requires U.S. companies to have a license before making any export or transfer to those companies. Thus, in the area of technology generally, with a significant impact on cyber technology, the United States and other governments are taking a greater management and monitoring role.

Conclusion

International economic tools already create and have created numerous intersections with cyber activity and the cross-border movement of cyber goods and services. This short primer has reviewed a large part of the territory in which these discussions are playing out. On the eve of a new decade, governments are likely to review and expand upon these preliminary engagements on an ever-changing area of technology and law.

References

- ASEAN (2018a) *Regional Comprehensive Economic Partnership*. Available from: https://asean.org/?static_post=rcep-regional-comprehensive-economic-partnership [accessed 21 May 2019].
- ASEAN (2018b) *Joint Leaders' Statement on the Negotiations for the Regional Comprehensive Economic Partnership (RCEP)*. Available from: https://asean.org/storage/2017/11/RCEP-Summit_Leaders-Joint-Statement-FINAL1.pdf [accessed 21 May 2019].
- Bacchus, J. (2017) How to take on China without starting a trade war. *Wall Street Journal: Opinion*.
- Bechky, P.S. (2018) Sanctions and the blurred boundaries of international economic law. *Missouri Law Review*. 83(1): 1–38.
- Claussen, K. (2018) Beyond Norms: Using International Economic Law Tools to Deter Malicious State-sponsored Cyber Activities. *Temple International & Comparative Law Journal*. 32: 113–134.
- Claussen, K. (2019) The Other Trade War. *Minnesota Law Review Headnotes*. 103:1–19.
- Cohen, S. & Morril, M. (2017) A call to cyberarms: The international arbitrator's duty to avoid digital intrusion. *Fordham International Law Journal*. 40(3): 981–1021.
- Committee on Technical Barriers to Trade (2018) *Minutes of the Meeting of 21–22 March 2018*. WTO Doc. G/TBT/M/74. Available from: https://docs.wto.org/dol2fe/Pages/FE_Search/DDFDocuments/245264/q/G/TBT/M74.pdf [accessed 21 May 2019].
- Council for Trade in Services (2017) *Communication from the United States: Measures Adopted and Under Development by China Relating to Its Cybersecurity Law*. WTO Doc. S/C/W/374. Available from: <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/W374.pdf> [accessed 21 May 2019].
- Debevoise & Plimpton (2017) *Protocol To Promote Cybersecurity in International Arbitration*. Available from: www.debevoise.com/~media/files/capabilities/cybersecurity/protocol_cybersecurity_intl_arb_july2017.pdf [accessed 22 May 2019].
- EC-Council: CISO Program (2018) *ASEAN Cyber Security Summit*. Available from: <https://ciso.eccouncil.org/portfolio/asean-cyber-security-summit/> [accessed 21 May 2019].
- European Commission (2017) Trade in Services Agreement (TiSA). Available from: <http://ec.europa.eu/trade/policy/in-focus/tisa/> [accessed 21 May 2019].
- Fidler, D. (2013) Economic cyber espionage and international law: Controversies involving government acquisition of trade secrets through cyber technologies. *ASIL Insights*. 17(10). Available from: www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving [accessed 21 May 2019].

- Friedman, A.A. (2013) *Cybersecurity and Trade: National Policies, Global and Local Consequences*. Center for Technology Innovation at the Brookings Institution.
- Information Technology Industry Council (2017) *Forced Localization*. Available from: www.google.com/search?q=inurl%3Ahttps%3A%2F%2Fwww.itic.org%2Fpolicy%2Fforced-localization&rlz=1C1GCEA_enUS850US850&oq=inurl%3Ahttps%3A%2F%2Fwww.itic.org%2Fpolicy%2Fforced-localization&aqs=chrome..69i57j69i58.2232j1j9&sourceid=chrome&ie=UTF-8 [accessed 21 May 2019].
- International Bar Association (2018) *Cyber Security Guidelines*. Available from: www.ibanet.org/LPRU/cybersecurity-guidelines.aspx [accessed 22 May 2019].
- International Centre for Settlement of Investment Disputes (2011) *OPIC Karimum Corporation v. The Bolivarian Republic of Venezuela: Decision on the Proposal to Disqualify Professor Philippe Sands, Arbitration*. ICSID Case No. ARB/10/14. Washington, DC, International Centre for Settlement of Investment Disputes. ¶23. Available from: www.italaw.com/sites/default/files/case-documents/ita0588.pdf [accessed 22 May 2019].
- International Centre for Settlement of Investment Disputes (2013) *Kiliç İnşaat İhale İhracat Sanayi Ve Ticaret Anonim Şirketi v. Turkmenistan: Award*. ICSID Case No. ARB/10/1. Washington, DC, International Centre for Settlement of Investment Disputes. ¶4.3.16. Available from: www.italaw.com/sites/default/files/case-documents/italaw1515_0.pdf [accessed 22 May 2019].
- International Centre for Settlement of Investment Disputes (2014) *ConocoPhillips Petrozuata B.V., ConocoPhillips Hamaca B.V. and ConocoPhillips Gulf of Paria B.V. v. Bolivarian Republic of Venezuela: Dissenting Opinion of Georges Abi-Saab*. ICSID Case No. ARB/07/30. Washington, DC, International Centre for Settlement of Investment Disputes. ¶1. Available from: www.italaw.com/sites/default/files/case-documents/italaw3121.pdf [accessed 22 May 2019].
- International Centre for Settlement of Investment Disputes (2017) *Caratube International Oil Company LLP and Mr. Devincci Salah Hourani v. Republic of Kazakhstan: Award*. ICSID Case No. ARB/13/13. Washington, DC, International Centre for Settlement of Investment Disputes. Available from: www.italaw.com/sites/default/files/case-documents/italaw9324.pdf [accessed 22 May 2019].
- International Centre for Settlement of Investment Disputes (2018) *Libananco Holdings Co. Limited v. Republic of Turkey: Decision Preliminary Issues*. ICSID Case No. ARB/06/8. Washington, DC, International Centre for Settlement of Investment Disputes. ¶82. Available from: www.italaw.com/sites/default/files/case-documents/ita0465.pdf [accessed 22 May 2019].
- International Council for Commercial Arbitration, the International Institute for Conflict Prevention and Resolution & the New York City Bar Association (2018) *Draft Cybersecurity Protocol for International Arbitration Consultation Draft*. Available from: www.arbitration-icca.org/media/10/43322709923070/draft_cybersecurity_protocol_final_10_april.pdf [accessed 22 May 2019].
- John, B. (2016) Admissibility of improperly obtained data as evidence in international arbitration proceedings. *Kluwer Arbitration Blog*. Available from <http://arbitrationblog.kluwerarbitration.com/2016/09/28/admissibility-of-improperly-obtained-data-as-evidence-in-international-arbitration-proceedings/> [accessed 22 May 2019].
- Mirasola, C. (2018) An update on Chinese cybersecurity and the WTO. *Lawfare*. Available from: www.lawfareblog.com/update-chinese-cybersecurity-and-wto [accessed 21 May 2019].
- Ortiz, R.C. (2018). Admissibility of hacked emails as evidence in arbitration. *NYU Law: Transnational Notes*. Available from: <https://blogs.law.nyu.edu/transnational/2018/05/admissibility-of-hacked-emails-as-evidence-in-arbitration/> [accessed 22 May 2019].
- Pastore, J. (2017) Practical Approaches to Cybersecurity in Arbitration. *Fordham International Law Journal*. 40(3):1023–1031.
- Ross, A. (2015) Tribunal rules on admissibility of hacked Kazakh emails. *Kluwer Arbitration Blog*. Available from: <https://globalarbitrationreview.com/article/1034787/tribunal-rules-on-admissibility-of-hacked-kazakh-emails> [accessed 22 May 2019].
- Shehata, I.M.N. (2018) Three potential imminent benefits of blockchain for international arbitration: Cybersecurity, confidentiality & efficiency. *Young Arbitration Review*.
- United States of America Department of State (2012) *2012 US Model Bilateral Investment Treaty*. Available from: <https://ustr.gov/sites/default/files/BIT%20text%20for%20ACIEP%20Meeting.pdf> [accessed 22 May 2019].
- United States of America Executive Office of the President (2015) *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*. Executive Order 13694. Washington, DC,

- Federal Register. Available from: www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities [accessed 22 May 2019].
- United States of America Executive Office of the President (2017) *Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities*. Executive Order 13757. Washington, DC, Federal Register. Available from: www.federalregister.gov/documents/2017/01/03/2016-31922/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious [accessed 22 May 2019].
- United States of America Executive Office of the President (2018) *Actions by the United States Related to the Section 301 Investigation of China's Laws, Policies, Practices, or Actions Related to Technology Transfer, Intellectual Property, and Innovation*. 83 FR 13099. Washington, DC, Federal Register. Available from: www.federalregister.gov/documents/2018/03/27/2018-06304/actions-by-the-united-states-related-to-the-section-301-investigation-of-chinas-laws-policies [accessed 22 May 2019].
- United States of America *International Economic Powers Act* (1977) 50 USC. §§ 1701–06. Washington, DC.
- United States of America The White House (2018) *Notice Regarding the Continuation of the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities*. Washington, DC, The White House. Available from: www.whitehouse.gov/presidential-actions/notice-regarding-continuation-national-emergency-respect-significant-malicious-cyber-enabled-activities/ [accessed 22 May 2019].
- World Trade Organization (2004) *Legal Effect of Panel and Appellate Body Reports and DSB Recommendations and Rulings*. Available from: www.wto.org/english/tratop_e/dispu_e/dispu_settlement_cbt_e/c7s1p1_e.htm [accessed 21 May 2019].
- World Trade Organization (2017a) *The WTO*. Available from: www.wto.org/english/thewto_e/thewto_e.htm [accessed 21 May 2019].
- World Trade Organization (2017b) *Members Debate Cyber Security and Chemicals at Technical Barriers to Trade Committee*. Available from: www.wto.org/english/news_e/news17_e/tbt_20jun17_e.htm [accessed 21 May 2019].
- World Trade Organization (2017c) *WTO Members Examine New Proposals for Domestic Regulation in Services*. Available from: www.wto.org/english/news_e/news17_e/serv_11jul17_e.htm [accessed 21 May 2019].
- World Trade Organization (2018) *Archive of Specific Trade Concerns*. Available from: www.wto.org/english/news_e/news18_e/tbt_21jun18_e_trade_concerns_e.pdf [accessed 21 May 2019].
- World Trade Organization (undated) *Dispute Settlement*. Available from: www.wto.org/english/tratop_e/dispu_e/dispu_e.htm [accessed 21 May 2019].

THE ROLE OF THE UN SECURITY COUNCIL IN CYBERSECURITY

International peace and security in the digital age

Eneken Tikk and Niels Nagelhus Schia

On the 75th anniversary of the United Nations, the UN Security Council is faced with difficult questions about its efficacy, relevance, and legitimacy. The leading powers and the permanent members (P5) of the Security Council – China, France, Russia, the UK and the USA – are drawn into a heavy contest over the world order. Power lines are (to be) drawn in an increasingly digital, interconnected and multi-stakeholder society. So far, despite the language from heads of states, global media houses and from leaders of international organizations, including NATO and the UN, none of the P5 countries has brought cyber to the UNSC. Other countries – for instance, Lithuania and the Netherlands – have considered introducing cybersecurity issues to the Council, but no action has followed. One of the most recent members-elect, Estonia, has pledged to take up the issue.

To stay relevant and act upon its responsibility for international peace and security, the Security Council will have to establish itself vis-à-vis cyber issues. The goal of this chapter is to examine why and how. To what extent do questions pertaining to digital threats and cybersecurity fall within the mandate of the Council and what could it address given the politically tense times among the P5? The analysis of the role of the UNSC in cybersecurity seems to be a blind spot in scholarly literature on international peace and security. Recently, leading scholars took stock of the relevance of the UNSC and its most pressing challenges in the twenty-first century in an edited volume of one thousand pages (von Einsiedel et al., 2016). However, neither information and communication technology nor cybersecurity are mentioned anywhere in that volume.

Essential to the discussion of the possible role of the Security Council in cybersecurity is how current international cyber affairs will be qualified in the context of the UNSC mandate: have contemporary uses of ICTs emerged as significant, new and urgent threat to the peace (Simma, 2012, p. 785)? Are there any disputes present among UN member states that, if continued, are likely to endanger the maintenance of peace (UN Charter, 1945, Art. 33)? Is the time ripe for the Council to consider ‘all things digital’ (Kaljulaid, 2018)? If so, despite the known limitations on its operability, a number of ways are open for the Council to become engaged. If not, any direct role of the Security Council must be dismissed. In this case, however, one must critically (re-)assess the relevance of the whole UN First Committee cybersecurity dialogue that is premised on the potential threat to international peace and security resulting from state use of ICTs.

Taking a stand on an issue beyond any particular territory or event is not unprecedented. With Resolutions 1373 and 1540 the Security Council addressed a more general and abstract issue that has led some authors to conclude that the Council has assumed a law-making role. By declaring international terrorism as a threat to international peace, the Security Council imposed general obligations on all States in a context not limited to a particular country (de la Serna Galvan, 2011, p. 148).

After a discussion of the current cybersecurity situation, we will proceed with a verdict on ICTs as a threat to peace and security, calling for a corresponding conversation between states, potentially at an invitation of a Security Council member state. The chapter continues with a discussion of ways in which the Security Council could become involved in matters of cybersecurity, briefly discussing likely applicable factors of limited operability. Finally, some related considerations for states are put forward.

Three outlooks on peace

The UNSC is the executive decision-making arena of the United Nations and the world's most important international decision-making body with the primary responsibility of maintaining international peace and security. The Council's legitimacy depends on the maintenance of its original purpose as set out in the UN Charter which, as Fassbender (2012) notes, is hard to verify or falsify. What characterizes this body is not only that its decisions have far-reaching effects across the world, but also that its decision-making process is affected by both the macroeconomics of power and the micro-politics of the informal processes (Schia, 2017, p. 55 and 2018, p. 122). This means that its effectiveness in decision-making is highly dependent of the climate between the Permanent Members.

After a honeymoon period from 1945 to the mid-1950s, the Security Council froze in the icy relationship between the United States and the Soviet Union. In the Cold War reading, of which the U2 incident and the Cuban Missile Crisis offer illustrations, the Security Council's role in world politics remained modest and passive. Wuthnow (2011) notes that since the fall of the Berlin Wall, the Council has met three times as often as it did during the Cold War. During the same period, it passed more than ten times more resolutions under Chapter VII than it did between 1946 and 1989 (Wuthnow, 2011, p. 4). The '1962 Outlook' on the Security Council would involve low expectations, where the Council remained largely detached from the world affairs and would not be seen as a source of inspiration for peace and stability. Fassbender summarizes that the expectations of the Security Council were so low that doing nothing was an achievement on its own (Fassbender, 2012, p. 53).

After the Cold War, new kinds of conflicts and broader security concerns were increasingly included on the Security Council agenda, many of them without immediate peace and security implications. The Security Council became regarded as a forum to uphold the purposes and principles of the UN, as enshrined in the UN Charter or the 1970 Friendly Relations Declaration. The '1992 outlook' has the Security Council both removing and preventing threats to peace, thereby occupying the most encompassing, powerful, and direct mandate to shape stability and order in the world. The Council has demonstrable achievements to feed such high expectations. In the context of the protection of civilians, the Council recognized 'the importance of a comprehensive, coherent and action-oriented approach, including in early planning, of protection of civilians in situations of armed conflict' and stressed

the need to adopt a broad strategy of conflict prevention, which addresses the root causes of armed conflict in a comprehensive manner in order to enhance the protection of civilians on a long-term basis, including by promoting sustainable development, poverty eradication, national reconciliation, good governance, democracy, the rule of law and respect for and protection of human rights.

(S/RES/1738)

Furthermore, the Council became concerned about ‘deliberate attacks in violation of international humanitarian law’ (S/RES/1738), stating that states “bear the primary responsibility to respect and ensure the human rights of their citizens, as well as other individuals within their territory as provided for by relevant international law’ (S/RES/2150). It put up strong opposition to impunity for serious violations of international humanitarian law and human rights law and emphasized the responsibility of States to comply with their relevant obligations to end impunity (S/RES/2150). Naturally, these lines remain in the context of the Security Council’s mandate. However, they leave little question as to the Council’s attitude towards international law, wherever it becomes seized of the matter.

More recent years, however, have shown new signs of an inefficient Security Council and a suboptimal working climate between its permanent members. Tensions have escalated with the civil war in Syria, the annexation of Crimea, accusations of interference in national elections and a combination of trade war, power politics, and old school geopolitics. The UNSC has not only become characterized by a difficult working atmosphere, but there is also a new trend in international relations, whereby decisions about international peace and security are being taken outside of the UN and there is an ‘emerging reality that the most important challenge to international peace and security is one in which the Security Council is not present, and arguably not relevant’ (Jones 2016, p. 802–804).

As superpower rivalry deepens, the question of the Council’s efficacy re-emerges. Several attempts have been made, without success, over the past years to make the Council more inclusive and better responsive to the international community’s needs (Simma, 2012; Fassbender, 2012). Alongside the expectations that have been made possible by the nearly 25 years of active involvement, the Council must face criticism about having become a vehicle for the USA and its allies to seek to punish and coerce regimes with which Russia and China maintain close relations (Wuthnow, 2011, p. 5). Similarly, Russia and China can be criticized for emphasizing hard security and absolute sovereignty over human security and human rights. Accustomed to the absence of hard conflict, the international community requires leadership in maintaining peace. It is unclear, both in the context of cybersecurity as well as in general security affairs, whether the Security Council will rise to this task.

In any case, the 1962 outlook, based on the realities of the Cold War, hardly satisfies the hopes of the international community of 2022. The 1992 outlook, in contrast, may put too high hopes on the Council. The central question in this chapter is the position that the Security Council could assume in international cyber affairs.

International cyber affairs in the context of peace and security

The (hypothetical) threat and the (quasi-) conflict

The question of the Council’s involvement is more than open. When looking at statements relating to cyber threats, it is not unreasonable to assume an active role of the UN Security Council in international cyber affairs. The General Assembly has called on UN member

states ‘to be guided in their use of recommendations of the Group of Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security’ (A/RES/71/28, para 1a). According to this report, ‘[t]he use of ICTs in future conflicts between States is becoming more likely’, ‘[t]he risk of harmful ICT attacks against critical infrastructure is both real and serious’ and states are ‘rightfully concerned about the danger of destabilizing misperceptions, the potential for conflict and the possibility of harm to their citizens, property and economy’ deriving from the difficulty of attributing the source of an ICT incident (UN A/70/174, paras 4, 5 and 7). Table 30.1 summarizes the argumentation (and consensus) on threats that uses of ICTs *may* pose to international peace and security in the three GGE reports.

However, this table contains a number of hypotheticals and the lack of any definitive action to follow up on these innovations. The GGE has iterated several times that the growing use of ICTs in critical infrastructures creates new vulnerabilities and opportunities for disruption, as does the growing use of mobile communications devices and web-run services. As the GGE in 2013 concluded, ‘any ICT device can be the source or the target of misuse’. The Group identified global connectivity, vulnerable technologies and anonymity as facilitators of the use of ICTs for disruptive activities. It noted that the ‘rapid increase in the use of mobile communications devices, web services, social networks and cloud computing services expands the challenges to security’ (GGE, 2013). Despite these pointers, the Group has not warned about the growing dependence on ICTs.

Furthermore, the Group has expressed concern that the ICT supply chain could be influenced or subverted in ways that would affect the normal, secure, and reliable use of ICTs. The inclusion of malicious hidden functions in ICTs can undermine confidence in products and services, erode trust in commerce and affect national security (GGE, 2010, p. 8). Not much has been undertaken to build or restore this trust.

In addition to the UN GGE, the Secretary-General has elaborated the cyber threat. In his address to the General Assembly in 2017 Secretary-General Antonio Guterres referred to cyber war as ‘a less and less a hidden reality – and more and more able to disrupt relations among States and destroy some of the structures and systems of modern life’ (United Nations Secretary-General, 2019). NATO’s Secretary-General Jens Stoltenberg also highlighted that cyber-attacks could be ‘as damaging as conventional attacks’, susceptible of ‘inflicting billions of dollars’ worth of damage to our economies, bring global companies to a standstill, paralyze our critical infrastructure, undermine our democracies and have a crippling impact on military capabilities’ (Stoltenberg, 2019). Joseph S. Nye highlights how the potential attack surface will expand dramatically and provide opportunities for both private and inter-state conflict (Nye, 2018, p. 7).

Despite the strong language pointing to international peace and security concerns, neither the UN GGE nor any other actor has been able to assert, in the context of state uses of ICTs, the acuteness of the politico-military threat, let alone a threat to international peace and security, breach of the peace or act of aggression that the UN Charter points to. Importantly, none of the states participating in the GGE has deemed it necessary to bring the issue to the UN Security Council.

It is equally problematic to discern immediate peace and security concerns from known or alleged state-sponsored cyber operations. Of known or allegedly state-sponsored cyber operations, the vast majority are cyber espionage. The rest, around 10% of all the catalogued incidents, have relatively low effects, such as website defacement, denial of service, in some cases data manipulation and, in a very few cases, sabotage and physical damage (Council of Foreign Relations. 2019; CSIS (2019); Maness, Valeriano and Jensen, 2019).

Table 30.1 Summary of the UN GGE 2010, 2013 and 2015 reports argumentation of the threats

2010	2013	2015
Thus far, there are few indications of terrorist attempts to compromise or disable ICT infrastructure or to execute operations using ICTs, although they may intensify in the future.	<p>The absence of common understandings on acceptable state behaviour with regard to the use of ICTs increases the risk to international peace and security.</p> <p>Terrorist groups use ICTs to communicate, collect information, recruit, organize, plan and coordinate attacks, promote their ideas and actions and solicit funding. If such groups acquire attack tools, they could carry out disruptive ICT activities</p>	<p>There are disturbing trends in the global ICT environment, including a dramatic increase in incidents involving the malicious use of ICTs by state and non-state actors.</p> <p>The use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security.</p>
There is increased reporting that states are developing ICTs as instruments of warfare and intelligence, and for political purposes. Uncertainty regarding attribution and the absence of common understanding regarding acceptable State behaviour may create the risk of instability and misperception		<p>A number of states are developing ICT capabilities for military purposes. The use of ICTs in future conflicts between States is becoming more likely.</p>
The growing use of ICTs in critical infrastructures creates new vulnerabilities and opportunities for disruption, as does the growing use of mobile communications devices and web-run services.	<p>The expanding use of ICTs in critical infrastructures and industrial control systems creates new possibilities for disruption.</p>	<p>States are rightfully concerned about the danger of destabilizing misperceptions, the potential for conflict and the possibility of harm to their citizens, property and economy.</p> <p>The most harmful attacks using ICTs include those targeted against the critical infrastructure and associated information systems of a state. The risk of harmful ICT attacks against critical infrastructure is both real and serious.</p>
The inclusion of malicious hidden functions in ICTs can undermine confidence in products and services, erode trust in commerce and affect national security.	<p>The rapid increase in the use of mobile communications devices, web services, social networks and cloud computing services expands the challenges to security.</p> <p>States are concerned that embedding harmful hidden functions in ICTs could be used in ways that would affect secure and reliable ICT use and the ICT supply chain for products and services, erode trust in commerce and damage national security.</p>	

2010	2013	2015
<p>The varying degrees of ICT capacity and security among different States increases the vulnerability of the global network.</p> <p>Differences in national laws and practices may create challenges to achieving a secure and resilient digital environment.</p>	<p>Different levels of capacity for ICT security among different States can increase vulnerability in an interconnected world. Malicious actors exploit networks no matter where they are located. These vulnerabilities are amplified by disparities in national law, regulations and practices related to the use of ICTs.</p>	

Source: Authors' compilation from the reports

Furthermore, the vast majority of known incidents reflect established dyadic rivalries where, if anything, they point to a slight de-escalation in means and methods of politico-military confrontation.

Effect-creating cyber incidents that have taken place with some state involvement in the past two decades can be characterized primarily as low-intensity conflict. Originating in US military doctrine, it has analytical value in the context of cyber and hybrid warfare:

Low intensity conflict is a political-military confrontation between contending states or groups below conventional war and above the routine, peaceful competition among states. It frequently involves protracted struggles of competing principles and ideologies. Low intensity conflict ranges from subversion to the use of armed force. It is waged by a combination of means, employing political, economic, informational, and military instruments.

(United States of America, 1996).

Taylor (1988, pp. 5–6) characterizes low intensity conflict as a situation where

interests are contested; organized violence is used to effect or influence outcomes; all elements of national power are employed; the military dimension is employed primarily for its political, economic and informational effect; military violence is employed indirectly or limited by time and objective.

The fact that cyber operations often do not meet the predicted thresholds of doom and destruction, deserves special attention in the context of international peace and security. The question becomes whether, due to their relatively low effects, cyber incidents should be disqualified as 'conflict', or is the discussion of conflict to be extended to struggles that remain, perhaps deliberately, below the threshold of use of force, yet constitute a new trend in state power projection. Most cyber incidents with known or suspected state involvement have occurred under explicit or implicit endorsement of the permanent members of the UNSC.

What are the prospects?

Estonia, one of the newest additions to the Council, has flagged the question of cyber-security as part of their candidacy campaign. The President of the Republic of Estonia has expressed the intent to raise issues of cybersecurity:

all topics concerning cybersecurity and artificial intelligence must be brought to the Security Council's table. Because the international legal space is showing a clear developmental delay in the field.... Estonia is planning to make a contribution namely to finding a solution to problems concerning cyberthreats.

(Kaljulaid, 2018)

The Estonian President has further elaborated on the plan, addressing the 73rd Session of the UN General Assembly:

Small countries have no time for small objectives – our aim is, among other issues, to bring all things digital to Security Council – cyber risks are something Estonians as citizens of a fully digitized state understand better than most. We want to offer our perspective to make sure that human beings remain safe in this new world where cyber related threats compound with conventional ones.

(Kaljulaid, 2018)

Indeed, ICTs constitute a pervasive technology that underpins not just advances in areas like materials, space, nuclear and biotechnologies (UNGA 1990). ICTs are also central to economic, societal, political, and military controls. ICT's omnipresence makes the currently 4.4 billion users (that is, over half of the world's population) online both recipients and potential sources of potentially destabilizing and security-endangering use of ICTs. However, is that enough of a reason for the Security Council to get involved in the discussion?

Accomplishing the Estonian endeavour is a challenge. Moscow and Washington, the leading powers in the cyber arms control dialogue, have remained silent on this particular issue. Despite making clear and frequent references to the threats related to the proliferation and certain uses of ICTs, neither the Russian Federation nor the USA have deemed it necessary to bring the matter to the attention of the Council. After two decades of expert discussions and heavy emphasis on arms control, this flags up the question of the real urgency and acuteness of the cyber threat.

It is also well acknowledged that the P5 hold fundamentally different positions on key aspects of cybersecurity. While the US, UK, and France, in general, share the same views on cybersecurity, China and Russia take a different position. These differences revolve around control of information and questions pertaining to sovereignty. While China and Russia emphasize the rights for states to protect their 'cyberspace' and 'information and media spheres', Western states fear that such rights will be used to justify surveillance, censorship, and repression in authoritarian states. Thus, by taking cybersecurity to the UNSC, Western states share a fear of opening a Pandora's box where already established rights concerning freedom of speech and human rights may be weakened. (For further details, see Tikk and Kerttunen 2018.) Thus global cyber governance and the role of the UNSC seem to hobble by an increasingly contentious debate that are i) obscured by attribution difficulties and the low-intensity character of cyber incidents ii) made difficult by political disagreements between P5, and iii) by an obfuscated situation concerning what it is that needs to be governed, the data or how to use the Internet.

However, the prospect may be improving, especially since Russia has taken a step towards a 'cyber-UNGA' with the OEWG. Getting the Security Council interested in cybersecurity issues is more in alignment with US interests than Russian aspirations. With the threat being unclear, the Council can embark on the US-championed proposition that the use of ICTs is to be guided under international law, while it is harder to imagine an angle that would lead the Council support the proposition of *lex specialis*.

The elevated status of the P5, with veto rights and the ability to make binding decisions, may be hampering the Council from dealing with cybersecurity. A premature discussion in the UNSC could leave the P5 in the trenches, where China and Russia would welcome international regulations that strengthen cyber sovereignty, while the USA and the UK would be very cautious about such regulation. Ironically, compared to the OEWG, the UNGGE itself can be construed as a model of the Security Council: it involves experts from the P5 and, initially, it started out with the total of 15 members selected on the basis of equitable geographical distribution. As a 'light version' of the UNSC, the GGE could be an easier place to discuss new norms at a level without the commitments which are needed in order to reach consensus in the UNSC. But the recommendations of the GGE do have a stronger status than most other groups of experts in the UN as they have been endorsed by the Group of Twenty (G20). In this way, the discussions in the GGE could be regarded as a stepping stone towards a UNSC discussion.

Despite lacking a hard-grade threat factor, state-sponsored cyber incidents constitute an alarming practice. Attacks against critical infrastructure are particularly worrisome because societal and civilian life is dependent of those systems and services. Cyberattacks directed towards electric power grids and power supplies such as the attacks on Ukraine in 2015 and 2016 may knock power offline and in turn knock out businesses and other vital societal systems. The second category concerns telecommunications. If telecommunications are turned offline or made inaccessible, the Internet will be offline and there will be no free flow of commodities and services – again businesses and other vital societal systems will be impaired. This has also been used by authoritarian regimes to control the public during politically sensitive events such as the 2010 election in Myanmar and the election in DR Congo in 2018. An example is also a ransomware attack on Baltimore's city government in the USA in May 2019, where EternalBlue, also used in WannaCry and NotPetya, shut down emails and systems allowing citizens to pay water bills, purchase homes, etc. The third category of attacks concern international financial systems like SWIFT (Society for Worldwide Interbank Financial Telecommunication) which interconnect banks around the world. During a series of cyberattacks on the SWIFT banking network in 2015 and 2016, millions of dollars were stolen, including a 101 million theft from the Bangladesh central bank. Through cyberattacks on global financial systems, banks that have taken the necessary security precautions may also become compromised through smaller banks in countries with lower standards on cybersecurity, national policy, and regulations. What is common in these attacks is that they hit the nervous and life-sustaining systems of modern societies: they disturb the anticipated and vital flows of information, literally, and goods and services. They can also destabilize peaceful international relations and can escalate existing conflicts.

Of further potential is a discussion of threats to democracy manifested in manipulation of democratic processes. The Council has, in past decades, adopted resolutions about the restoration of democracy (S/RES/948), endorsing the results of free and fair elections (S/RES/960), civilian policing (S/RES/1212), and facilitating a comprehensive political dialogue (S/RES/1040). Whether the development or uses of ICTs constitute a threat to the peace or endanger the maintenance of the peace, is the main question of this book that cannot be resolved on the basis of the evidence and claims presented so far. It remains subject

to further debate on whether the international community is willing to tolerate the economic and political struggles between the USA and its allies on the one side, and the Russian Federation and China on the other. As seen from the permanent members' perspective, such struggles should be considered normal in contemporary world politics. Whether others agree, remains to be discussed. There are several ways for the Security Council to become part of this conversation.

There are also some precedents for the theme being discussed under the aegis of the Council. Spain and Senegal made an attempt in November 2016 to get the Council involved in cyber security beyond the terrorism-related resolutions where cyber security is increasingly incorporated. They initiated and chaired an open Arria-meeting on cyber security – these are informal meetings the UNSC can arrange, mainly to meet with other delegations or NGOs or special representatives, and to discuss topics in a less binding manner.

The 2016 meeting included governments, organizations, civil society, and the private sector and sought to broaden the UNSC discussion on the matter by focusing on states and their potential use of cyberattacks and ICTs in political or military tensions, as well as the need to protect ICT-dependent critical infrastructure (What's in Blue, 2016; UNIDIR 2017, p. 25). At this meeting Council members were encouraged to improve ways of assessing vulnerabilities and preventing cyberattacks, to develop national strategies and policies, to commit to international cooperation, and to emphasize multi-stakeholder partnerships. Furthermore, the Arria-meeting questioned whether the Council itself was receiving appropriate information on two important aspects: i) on how ICTs can be used in emerging political and military tensions; and ii) on how the Council can contribute to mitigating these security implications.

In 2017, another ICT-related Arria-meeting was held, this time on 'hybrid wars as a threat to international peace and security'. The meeting was chaired by Ukraine and included discussions on cyber technologies, interference with political processes, disinformation and international peace and security (UNIDIR 2017, p. 25). Further, the UNSC's work on counter-terrorism there has been some aspects pertaining to ICTs included in resolutions. Resolutions 1267 (1999) and 1373 (2001) which constitute the framework for this work explicitly mentions terrorist use of ICTs (UNIDIR 2017, pp. 38–42).

Considerations for governments

None of the permanent members has taken the cybersecurity issue to the Security Council, despite their deep investment in the cyber arms control dialogue for over two decades. While changes in the attitudes of some of the P5, especially China and France, cannot be ruled out, it is more likely that the issue of cybersecurity ends up in the Security Council Chamber via a non-permanent member, another UN member state, the General Assembly or the UN Secretary-General. Without much prospect of the permanent members taking up the issue, it falls upon all interested governments to develop a convincing account of the Security Council's role and the expected outcome of its involvement.

The permanent members are split in their views about the role of ICTs in social, economic, political, and military affairs. Consequently, informal consultations and meetings are a more fruitful way ahead, at least in the coming two years where the new UN GGE and OEWG are in session. Whether the P5 will stand up to a sense of shared stewardship and global responsibility, being potentially accepted as the world police, remains to be seen. Meanwhile, as long as the rest of the world acts like the periphery, they will be treated as such. Breaking the empty cycle of cyber talks requires strong leadership and strategic vision,

which can be developed gradually via a series of examinations of state uses of ICTs, their implications as well as underlying causes, to decide whether and how any of these do or can endanger peace.

The Open-Ended Working Group that parallels the UN GGE has been dubbed the cyber-UNGA (Krutskikh 2019). The General Assembly remains a forum for states to draw attention to ongoing cyber incidents as well as trends in the state development and use of ICTs. A worthwhile exercise for all governments interested in the progress of international cybersecurity solutions is to consider whether the UN GGE has been run as a suboptimal substitute to the UN Security Council in this area. This question has both a substantive and a procedural element – by referring to cyber threats to peace and security as a hypothetical, while refraining from involving the Council in the matter, the GGE exercises factual control over the agenda. Procedurally, despite (or maybe because of) the lack of any authority, the GGE offers the P5 a viable alternative to bringing their views to the public. More importantly, however, the ‘cyber-UNGA’ offers a venue for serious discussion of the seriousness of the cyber threat. It must be asked whether the cyber threat should be considered and addressed independently or in conjunction with other, conventional or emerging security challenges.

It is therefore worth reminding ourselves that states are trust givers of the UNSC through the UN framework (Simma, 2012, p. 775) Under Article 11 of the UN Charter, the General Assembly has the power to call the attention of the UNSC to issues of international peace and security. The UNGA is instrumental in the selection of UNSC member states. Here, in addition to geographical distribution, aspiring member states’ contributions to international (cyber) peace and security could be considered. The UNGA is therefore well placed to take deeper interest in state uses of ICTs and the implications thereof to international peace and security.

Estonia might become the first state to open the cybersecurity chapter in the Security Council. After all, it is likely that the Council will conclude, like the GGE so far, that the use of ICTs is covered by international law. This would suit US interests as it would counter-balance the ‘cyber-UNGA’. However, is this approach going to engage the Council or not?

An obvious way for a question concerning certain uses of ICTs to be raised in Council is a devastating cyber incident with human casualties. Such scenarios have been predicted but state practice so far indicates restraint in this respect. Alternatively, the question may be framed in terms of a lasting situation that, if continued, may endanger the maintenance of peace. Here, any state invested in the issue of national and international cybersecurity, and sufficiently independent from the leading actors, is a potential pathfinder, mediator, and thought leader. The UN Secretary-General’s call for prevention and greater concern of the world’s well-being deserves attention in this context.

What the Security Council has to say about the use of ICTs would, of course, depend heavily on more specific framing of the issue. The P5 could take the high road by seeking agreement (and providing assurances to the world) in the dimension of strategic cybersecurity and stability. An example could be a discussion of the role of ICTs in nuclear security and a commitment to prevent the uses of ICTs in ways that would make possible inadvertent or deliberate use of the nuclear weapons.

Concluding thoughts

Any change starts with a vision for an alternative. Coming up with that vision requires a candid assessment of the current affairs – what, if anything, is wrong in state use of ICT? How can it be changed towards what is commonly seen as a viable and good alternative? What role can individual states, the Council and the P5 play in enabling, facilitating or actuating

this? These questions need answers before any reforms or agendas can be credibly tabled. Fassbender's observation of there being an agreement that the SC must be adapted to the present conditions of international life begs the question what those conditions are and what is there to be adapted. Individual states, NGOs, academia, and the private sector can offer views on what constitutes the cyber portion of international contestation, how to prevent cyber conflict and how best to mitigate incidents.

The challenge of escaping being famous for being (still) alive and reflecting how much, in fact, world affairs circle around five sovereign states, has nothing to do with cyber, as is the case with most of the contestation and conflict in today's world. More than anything, the Security Council is testament to the international community living a relatively comfortable life, while rogue actors and muscle states operate just shy of the thresholds for the use of force. The P5 need to realize that their actions and inactions do not set precedents just for the periphery but also for the international community they are part of. However, without a critical mass of international effort and determination, there will not be enough pressure in cybersecurity issue circles to make a decisive turn from threat narratives to systemic risk management, governance, and stewardship.

References

- Anon. (2019) Private conversations with high officials of the Russian Federation.
- Council of Foreign Relations (2019) Cyber Operations Tracker. Available from: www.cfr.org/interactive/cyber-operations [accessed 27 June 2019].
- von Einsiedel, S., Malone, D.M., and Stagno Ugarte, B. (eds) (2015) *The UN Security Council in the 21st Century*. Lynne Rienner, Boulder.
- Fassbender, B. (2012) The Security Council. In Cassese, A. *Realizing Utopia: The Future of International Law*. Oxford University Press, Oxford.
- Jones, B. (2016) The Security Council and the changing distribution of power. In von Einsiedel, S., Malone D., & Stagno Ugarte, B. (eds) (2016) *The Security Council in the 21st Century*. Lynne Rienner, London.
- Kaljulaid, K. (2018) Address by the President of the Republic of Estonia Kersti Kaljulaid at the 73rd United Nations General Assembly. Available from: www.president.ee/en/official-duties/speeches/14577-address-by-the-president-of-the-republic-of-estonia-kersti-kaljulaid-at-the-73rd-united-nations-general-assembly/index.html [accessed 28 June 2019].
- Krutskikh, A. (2018 and 2019). Speeches at the International Information Security Research Consortium conference. Garmisch-Partenkirchen (April 2018 and 2019) and Moscow (December 2018).
- Mancini, F. (2016) Promoting democracy. In von Einsiedel, S., Malone D., & Stagno Ugarte, B. (eds) (2016) *The Security Council in the 21st Century*. Lynne Rienner, London.
- Maness, R.C., Valeriano, B. & Jensen, B. (2019) The dyadic cyber incident and dispute data version 1.5. Available from: <https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset> [accessed 27 June 2019].
- Nye, J.S. (2018) Normative restraints on cyber conflict. Harvard Kennedy School, Belfer Center for Science and International Affairs.
- Schia, N.N. (2017) Horseshoe and Catwalk: Power, Complexity and Consensus-Making in the United Nations Security Council. In Niezen, R. and Sapignoli, M. *Palaces of Hope – The Anthropology of Global Organizations*. Cambridge University Press, Cambridge.
- Schia, N.N. (2018) *Franchised States and the Bureaucracy of Peace*. Palgrave Macmillan, London.
- Serna Galvan, M.L. de la (2011) Interpretation of article 39 of the UN Charter (Threat to the peace) by the Security Council. *Anuario Mexicano de Derecho Internacional*, XI, 147–185.
- Simma, B. (2012) *The Charter of the United Nations: A Commentary*. Oxford University Press, Oxford
- Stoltenberg, J. (2019) Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London. (May 23) Available from: www.nato.int/cps/en/natohq/opinions_166039.htm [accessed 23 August 2019].
- Taylor, R.H. (1988) What are these things called “operations short of war”? *Military Review*. 68.

- Tikk, E. & Kerttunen, M. (2018) *Parabasis: Cyber diplomacy in stalemate*. Norsk Utenrikspolitisk Institutt (NUPI). Available from: www.nupi.no/en/Publications/CRISTin-Pub/Parabasis-Cyber-diplomacy-in-Stalemate [accessed 27 June 2019].
- UNIDIR (2017) *The United Nations, Cyberspace and International Peace and Security – Responding to Complexity in the 21st Century*. UNIDIR Resources.
- United Nations (1945). *The Charter of the United Nations*.
- United Nations General Assembly (UNGA) (2016) Developments in the Field of Information and Telecommunications in the Context of International Security (9 December) A/RES/71/28.
- United Nations General Assembly (UNGA) (2010) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/65/201 (30 July)
- United Nations General Assembly (UNGA) (2013) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/68/98 (24 June)
- United Nations General Assembly (UNGA) (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174 (22 July)
- United Nations General Assembly (UNGA) (2018) *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/RES/73/27 (11 December)
- United Nations General Assembly (UNGA) (2019) *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. A/RES/73/266 (2 January)
- United Nations Secretary-General (2017) Secretary-General's Address to the General Assembly (December 17). Available from: www.un.org/sg/en/content/sg/statement/2017-09-19/secretary-generals-address-general-assembly [accessed 23 August 2019].
- United Nations Security Council (1994) Resolution 960 (29 January) S/RES/960
- United Nations Security Council (1994) Resolution 948 (15 October) S/RES/948
- United Nations Security Council (1996) Resolution 1040 (21 November) S/RES/960
- United Nations Security Council (1998) Resolution 1212 (26 November) S/RES/1212
- United Nations Security Council (1999) Resolution 1267 (15 October) S/RES/1267
- United Nations Security Council (2001) Resolution 1373 (28 September) S/RES/1373
- United Nations Security Council (2004) Resolution 1540 (28 April) S/RES/1540
- United Nations Security Council (2006) Resolution 2150 (16 April) S/RES/2150
- United Nations Security Council (2006) Resolution 1738 (23 December) S/RES/1738
- United States of America (1996), FM 100-20 Military operations in low intensity conflict. Available from: www.bits.de [accessed 27 June 2019].
- What's in Blue (2016) Open Arria-formula Meeting on Cybersecurity. Available from: www.whatsinblue.org/2016/11/open-arria-formula-meeting-on-cybersecurity.php [accessed 27 June 2019].
- Wuthnow, J. (2012) *Chinese Diplomacy and the UN Security Council: Beyond the Veto*. Routledge, London.

INTERNATIONAL LAW AND CYBER CONFLICT

*Gary D. Brown**

Introduction

It has long been an article of faith in the international legal community that international law, and international humanitarian law (IHL) in particular, would shield civilization from unrelenting cyber conflict. As cyberspace capabilities and the reliance of governments and civil society on the backbone of cyberspace to host communications, critical infrastructure, financial system, personal memories, military and intelligence records, etc, grew, there was an understanding that the complex system of international law built over past centuries was sufficiently robust to flex to this new challenge. One reason is the Martens Clause, which says in cases not addressed in the Hague Conventions warfare will continue to be subject to ‘the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of the public conscience’. Another is historical precedent. Lawyers noted that international law has successfully expanded to deal with emerging legal challenges related to air warfare, precision munitions, and noninternational armed conflict (NIAC). Surely, cyber warfare would be no different.

In the event, international law has proven less than adequate for the task. Despite increasing awareness of the threat and countless meetings, organizations, and publications devoted to the international legal system’s application to cyberspace, cyber-enabled aggression and conflict continues to grow. (ODNI, 2019, pp. 5–6) Looking back on the past two decades provides perspective to analyze international law’s shortcomings. Historical analogies offered to demonstrate the flexibility of international law fail to reflect just how different cyberspace operations are from previous developments. Commonly cited examples of IHL’s success in modernizing are, after all, merely straightforward applications of law to better ways of doing the same thing. Planes could be viewed as flying artillery, and precision munitions merely more accurate bombs. NIAC is just a legal classification of armed warfare. None of these

* The views expressed in this paper are those of the author and are not an official policy or position of the National Defense University, the Department of Defense or the US Government.

examples provides anything close to the fundamental challenge to the legal order presented by the advent of cyber operations.

The development most similar to cyberwarfare is lethal autonomous weapons systems (LAWS), but even this analogy is deeply flawed. Not only are LAWS a distant and less complicated cousin of cyberwarfare, it would be bold to conclude that law has adequately dealt even with the simpler case of LAWS. Some experts have concluded that LAWS are illegal in development and use, while others have concluded they are perfectly lawful and may be fielded immediately (Human Rights Watch, 2018; Press, 2018, p. 1337). When legal experts are able to support opposite conclusions on the legality of developing technologies, the coherence of the system is open to question.

One reason the analogy to cyber warfare breaks down in these cases is because the majority of competitive cyber activity is conducted at a level that does not implicate law governing armed conflict. Cyber aggression is largely occurring in the competitive ‘grey’ space between peace and war. States penetrate adversary systems and implant malware, disrupt systems without causing damage, manipulate data, etc. These activities are not clearly addressed under current international law.

Another reason kinetic – meaning physical rather than virtual – analogies are a poor fit is scale. Cyberspace activities can be conducted at a scale that is simply not possible in the physical world. The increase in data collection and analysis, as well as the digitization of data that in past decades would have been stored in physical form, has made the electronic transport of effectively all information transportable over data lines possible. The increase in Internet speed enables the transfer of large amounts of data almost instantaneously. That speed also means Internet aggression can occur at speeds far surpassing human ability to observe, much less orient, decide, or act, to complete military strategist John Boyd’s OODA loop (Coram, 2002). Boyd argued that adversaries’ rapid operations tend to force adversaries to make mistakes in war, because they lose the ability to follow the strategic process of observe, orient, decide, and act. That is, if one can get inside the enemy’s ‘OODA loop’, one will force errors and be likely to prevail as a result. Cyber operations have the potential to act far faster than anything seen before, potentially rendering human judgment irrelevant after the onset of hostilities. That is something not seen before, even in the case of air operations.

Finally, cyber malfeasance is often perpetrated by criminals not associated, or only loosely associated, with state governments. This, as well, is an underappreciated difference between cyberspace activities and other modes of interstate competition. Although criminals use some traditional weapons of war, they are not often found to be making use of fighter jets, precision-guided munitions, or (as yet) space and laws in their nefarious business. International law provides a theoretical framework to address state sponsorship of nonstate groups. However, the ability of cyber actors to conceal their location and identity, as well as the challenge of distinguishing purely criminal behaviour from state-sponsored activity, presents an unprecedented challenge.

Because of the ubiquity of cyberspace and Internet-connected devices, there is an extraordinary number of novel cyber-related legal issues. Reams have been written about law in the area, and this chapter serves as the briefest of introductions to some of them. It focuses on the application of general international law and the law of armed conflict. It also touches on the application of international human rights law (IHRL) to cyberspace operations, and efforts to control interstate cyber conflict through the development of international norms of behaviour.

Legal framework

Applying the international legal system to peacetime cyberspace highlights the system's ambiguities. Applying it to cyberwarfare creates something akin to chaos. International law relevant to cyberspace operations may be divided into general international law, including law governing the resort to war (*jus ad bellum*), and the law governing the conduct of armed hostilities (*jus in bello*). Even this general division of international law is not straightforward when applied to online activities.

Basic issues such as what constitutes a use of force or an armed attack – either of which could trigger armed conflict – or a violation of sovereignty are open questions in the cyber context. Normally, states falling victim to aggressive action are able to choose from a well-thumbed menu of appropriate and proportionate response options. Discover a spy ring? Expel diplomats and seize properties. Encounter unfair trading practices? Impose a tariff and levy sanctions. Suffer an invasion? Respond with a projection of armed force. Cyberspace is less orderly.

While in the physical world, the range of responses to various aggressive acts is understood, and mutual expectations tend to prevent miscalculation, in the realm of virtual activity, states must exercise discretion even in the categorization of the original 'act'. This means that with regard to cyberspace activities, states must deal with the risk of miscalculation in both reading the intent of the trigger and in formulating the response. Not only is there little practice on which to base predictions of state reactions to cyber-attacks or violations of cyber sovereignty, there is no consensus on exactly what cyber activity would constitute an attack or sovereignty violation. All of this, of course, is made even more confusing by the challenge of obtaining evidence sufficient to attribute aggressive cyber activities to a state with any certainty.

The combined lack of clarity in both original action and the response, combined with the difficulty in attributing actions to states, results in an uncertain environment for inter-state relations with regard to cyber activities. It is unclear how states view hacks of private entities, cyber penetrations of financial institutions, prepositioned malware on power grids, and cyber-enabled, state-sponsored disinformation campaigns, for example, much less how they might respond to them. There is no typology of cyber events, nor is there a grammar of escalation. A particularly vexing issue has been determining the extent to which the notion of sovereignty applies to cyber activities.

Sovereignty and unlawful intervention

The notion of sovereignty seems intuitive, but can be slippery in application. *Oppenheim's International Law* defines sovereignty as 'the supreme authority of every state within its territory' (Jennings & Watts, 1992). It is the connection of sovereignty to territory that provides the challenge in cyberspace.

While it is true the Internet is hosted on and facilitated by physical infrastructure, such as servers, cable, and routers, cyberspace has resisted attempts to pigeonhole it into standard notions of sovereignty, which is largely defined by physical territory. Normally, states are expected to assume responsibility for aggressive actions emanating from their territory. States have not been expected, by contrast, to assume full responsibility for cyber actions coming from inside their borders. Noxious cyber actions may be facilitated by equipment that happens to be located within a state's borders, but the state may have no inkling the activity is taking place. Cyber actions are likely to be hosted on commercial infrastructure,

and the government is often unaware of the details of commercial activities occurring on its territory. *Spamhaus Botnet Threat Report* (Spamhaus, 2017) reports that once again in 2018 the US hosted more botnet command and control servers than any other state. Russia is ranked second, and the Netherlands is third. If responsibility were determined solely by the origin of the cyber aggression, these three states would be accountable for over 50% of the world's malicious cyber events.

It is accepted that violating sovereignty is unlawful, but there are differing opinions regarding what actions constitute violations. Armed attacks and uses of force constitute violations of sovereignty. In the case of state-sponsored cyber operations having effects in another state but not rising to the level of armed attacks or uses of force, it is unclear whether they violate sovereignty. The UK's position, for example, is that there is no standalone violation of territorial sovereignty solely through cyber activity (Wright, 2018).

Espionage often violates sovereignty, but as a matter of practice, states treat spying as *sui generis*. A particular way a cyber operation could violate sovereignty is by violating the non-intervention principle.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Schmitt, 2017) Rule 66 states the principle succinctly: 'A State may not intervene, including by cyber means, in the internal or external affairs of another State'. This means states must refrain from coercively interfering in matters within another state's *domaine réservé*. The clearest example of a cyberspace-enabled violation of the nonintervention principle is interfering with another state's elections. The exact extent of a state's *domaine réservé* may vary over time, but the choice of a political system and its organization will always be matters of particular importance to a state. The UK noted its position that interference in the domestic affairs of another state is a violation of sovereignty, and specifically named interference with elections as a violation of the nonintervention principle (Wright, 2018).

To determine whether to consider the cyber activity of another state an instance of unlawful intervention, among other things a state might consider whether the offending cyber activity directly affected a government activity or system, and how critical or important that system is for the victim state. For example, the industrial control systems of nuclear power facilities are likely of critical concern, as is election infrastructure. Tourism and educational websites might not be considered as critical to government functioning. Cyber transgressions likely to have a significant negative effect on the target state's economy would more likely be considered coercive interventions. Future examples of events states consider, and do not consider, unlawful interventions will provide more detail on this question.

Use of force and armed attack

Although attempts to outlaw armed conflict, such as 1928's *Kellogg-Briand Pact*, have had little effect, since WWII states have agreed that force may only be used lawfully in self-defence or pursuant to UN resolution. The law governing the conditions under which states may resort to conflict with other states is captured in the UN Charter.

Two provisions of the UN Charter are of particular relevance to armed conflict, cyber or otherwise. One is Article 2(4). 'All member [states] shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state'. Determining what constitutes a use of force is sometimes challenging, but is relatively straightforward compared to analyzing whether cyber intrusions violated territorial integrity and exactly which cyber-enabled acts interfere with political independence.

The types of activities that violate the prohibition on the use of force under Article 2(4) are not entirely clear even with regard to physical activities. UN General Assembly Resolution 3314 lists examples of acts that would qualify as acts of aggression, including invading or attacking another state's territory, bombarding or using other weapons against the territory of another state, or attacking another state's armed forces (UNGA, 1974). These examples are not very helpful in determining whether trespass on computer networks or hostile communications to members of the armed forces, for example, would constitute uses of force.

Article 51 of the Charter sets out the customary right of states to defend against armed attacks. In 1986 the International Court of Justice (ICJ), in *Military and Paramilitary Activities in and against Nicaragua* (the *Nicaragua Case*), provided some texture to the words of Article 51 when it held that only the most grave uses of force qualify as armed attacks, suggesting an examination of the scale and effects of aggressions is necessary to determine whether they cross the armed attack threshold (ICJ, 1986, p. 101–104).

At least when actions clearly amount to aggressions in breach of international peace, states have a shared understanding the controlling legal framework. An area of growing concern for states is the lack of a clear line between noxious behaviour in cyberspace and a cyber use of force. A miscalculation by a state in this uncertain environment could lead to unintentional escalation from peacetime competition to armed conflict. States have been reticent about their cyber activities, only rarely admitting ownership of cyber operations, so there are few official statements to provide detail to help understand what states would read as escalatory. If the unwelcome actions of a state results in kinetic effects, it may be treated identically to a kinetic action having the same effect. This is set out in *Tallinn Manual 2.0*, Rule 69(8): 'Acts that injure or kill persons or physically damage or destroy objects are uses of force'. For example, the US has made clear that it cares little whether damage or destruction is caused by cyber or physical means, the aggression will be analyzed the same.

Actions falling short of this level are in an as-yet undefined grey zone. In the absence of state practice in the area, *Tallinn Manual 2.0* suggests several things states might consider when determining whether a nondestructive cyber operation crosses the use of force threshold. They include severity of the consequences, directness of the causality of the harm, and intrusion on areas of state interest, among several other factors (Rule 69(9)). The length of the list makes it unlikely states would be able to use it to drive their deliberations in real time; the factors are more suited for a *post facto* determination of a cyber event. In any event, although the listed factors reflect a logical assessment of which cyber operations states might find particularly offensive, other factors such as the relative strength of the players and domestic politics, for example, might drive states, as well. To date, scholars have little insight into the actual considerations of states. This uncertainty leaves open the possibilities of misreading intent and escalating conflict.

It is important to note that, even when the perceived aggression triggering the response is a cyber operation, there is no restriction on the method of response for lawful exercises of self-defence. Responses to cyber aggressions might be cyber-based, but could just as lawfully be traditional military actions, quickly escalating from a misread cyber intrusion to traditional warfare.

The Sony hack of 2014 illustrates the murky boundaries of cyberspace aggression. In that case, hackers virtually destroyed thousands of Sony's computers by wiping the hard drives and deleting the master boot records that would have made recovery of the deleted data feasible. They also stole and distributed confidential information and intellectual property belonging to Sony, all resulting in an estimated US\$70–100 million loss for the corporation (Richwine, 2014).

The US attributed the incident to North Korea. In the physical world, when state-on-state activity crosses the threshold of destruction, an armed response is considered. In this case, however, perhaps because the damage was virtual rather than physical, no lives were lost, and the victim was a commercial entity, the US elected to categorize the incident as cyber vandalism, and treat it as a crime rather than as an act of aggression (Holland & Chi-acu, 2014). It is possible, depending on the scale, that a state-sponsored kinetic event resulting in a similar amount of physical damage would have been treated as the opening salvo in an armed conflict. Despite this single precedent, in the future a state might treat a similar incident as an aggression meriting an armed response in self-defence. In the Sony case, the US had an apparently lawful option to respond forcefully to a use of force, but chose to characterize the triggering event as a crime.

Simply put, there is international law applicable to the area of cyber aggression, and expert commentary to interpret it, but current law does not prohibit most of the activities in which states are engaging. Further, even when state cyber misconduct amounts to a use of force, it is unclear whether states will generally interpret it as such. The continuing ambiguity in the area, caused partly by a lack of official public discourse, creates uncertainty about how international law will be applied to cyber operations. This, in turn, raises the possibility of accidental escalation of cyber conflict.

Retorsion and countermeasures

Although the majority of cyber misconduct occurs in the grey space below armed conflict, states falling victim to cyberspace misconduct in that category are not without lawful remedies. One of them is retorsion, which consists of lawful but unfriendly actions taken in response to unfriendly but lawful actions by another state. An example of retorsion is the expulsion of diplomats after a similar action by the offending state. A cyberspace example of retorsion might be squeezing the Internet bandwidth available to a particular state to slow its flow of Internet traffic for a time, in response to the offending state using its official web presence to distribute unflattering information about another state.

Retorsion is a time-tested model of international engagement. A more aggressive option, still short of armed conflict, is the notion of cyber countermeasures. A lawful countermeasure is a necessary and proportionate activity, illegal but for its status as a countermeasure, taken to end illegal activity by another state. Countermeasures must not themselves be armed attacks and cannot be retaliatory or anticipatory, although they may be employed to end a continuing campaign of unlawful activity. The notion of countermeasures is set out in *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (ILC, 2001) and the rule's application to cyberspace is discussed in *Tallinn Manual 2.0* (Rules 20–26).

Although most of the parameters of countermeasures are agreed upon by states, there is not universal understanding of every element. The *Draft Articles* indicate countermeasures that would be uses of force are not permitted, and that notice of intent to engage in countermeasures must be given. (ILC, 2001, Arts.50 and 52). However, some states do not concur with these two requirements (*TM 2.0*, Rule 22(10–113); Wright, 2018).

Iran's response to the Stuxnet incident, while not an ideal exemplar of countermeasures, helps illustrate the elements of the concept. It is one of the few cases providing enough public detail to study. In 2010, the Stuxnet worm infiltrated numerous computer systems around the world, eventually gaining access to the industrial control system at Iran's uranium enrichment facility at Natanz. Once the worm was in place at Natanz, it carried out a cyber-attack against the facility. Although Iran did not release specific details regarding the effects of the

attack, estimates were that the Stuxnet worm destroyed about 1,000 uranium enrichment centrifuges (Holloway, 2015). Despite a number of media reports assigning responsibility for Stuxnet to the US and Israel, Iran, for its own reasons, chose not to treat Stuxnet as act of international aggression. Rather, Iran appears to have treated the Stuxnet attack as illegal activity that fell short of a use of force. Iran made no public statements on countermeasures, but apparently responded to the incident with a wide-ranging campaign against the US banking system. Iran's actions resemble a countermeasure. If Iran determined Stuxnet was part of an on-going campaign, then it could assert its actions were a necessary and proportionate response to end aggression against a system vital to its national security. If, on the other hand, Stuxnet was an isolated incident and not part of an on-going campaign, Iran's actions fail as a countermeasure because they were for a punitive or retributive purpose.

If states are driven over the threshold of armed conflict by cyberspace or other aggressive activity, international humanitarian law (IHL) takes effect. IHL has been a unique area of international cooperation over the years. Warring states able to agree on little else have generally agreed that warfare should be conducted within certain bounds of humanity, in order to minimize impact on civilian, noncombatant communities. IHL provides a framework for that protection, while still allowing states to wage war. Even this robust body of law, however, presents challenges in its application to cyberspace activities.

International humanitarian law

In the ambiguous and often ill-defined world of international law, IHL is a cornerstone. As discussed above, however, it is not a simple matter to determine when cyber competition becomes armed conflict. Even when states are indisputably involved in an armed conflict, application of the normally straightforward principles of IHL to virtual operations and effects is difficult.

IHL can be summarized in four principles: humanity, necessity, proportionality, and distinction (ICRC, 2019). In the most basic sense, the principles require combatants to avoid using methods of warfare that cause unnecessary suffering; to attack only when necessary; to ensure that anticipated collateral damage and injury do not outweigh anticipated military gain from an attack; and to ensure that only appropriate targets are the object of attack. The application of these principles to cyber operations resulting in kinetic effects is clear because the effect is measured rather than the means. Whether a transformer is destroyed with a grenade or a computer virus, or whether a bridge is dropped by a bomb or by destructive malware, is irrelevant under IHL.

Under existing law, it is unclear how to determine whether nefarious yet nondestructive cyber activity during armed conflict constitutes an attack. This is a critical determination because, although IHL applies to all activities in armed conflict, the primary regulatory principles attach on attack. Sub-attack (i.e., non-kinetic) cyber aggression in the context of armed conflict does not trigger application of the major principles of IHL. The principle of distinction requires parties to a conflict to refrain from making the civilian population and civilian property the object of *attacks*. The rule of proportionality prohibits *attacks* which may be expected to cause incidental civilian death or injury, or damage to civilian property which would be excessive in relation to the concrete and direct military advantage anticipated. The principle of distinction does not require that activities other than attacks distinguish between civilian and military 'targets'. For example, reconnaissance can be directed at civilian objects in wartime without violating the principle of distinction. Similarly, no proportionality assessment is required for actions in the context of armed conflict that are not attacks.

On-line activities directed against the Republic of Georgia illustrate how IHL applies to cyber actions during armed conflict. During the Russian invasion of Georgia in 2008, it is widely reported that cyber actors in Russia engaged in denial-of-service attacks against both government and civilian targets in Georgia. The effect of the cyber-attack was to make web-sites and online services unavailable for a period of time. The targets included financial institutions, communications forums, news media, and public facing government sites. (Tikk, Kaska & Vihul, 2010, pp. 66–90). The actions were taken in the course of an armed conflict so IHL applied. Even though many of the targeted sites were civilian, the cyber operations were not prohibited because the operations were mere disruptions and not attacks.

In Syria, too, cyberspace has paid a significant role in the armed conflict. The effects there have most been seen through the use of cyber-enabled communications. The dominant role social media has played in providing information about the conflict has resulted in distorted perspectives on the situation, and has provided both sides the opportunity to manipulate the 'facts' to suit its perspective. The conflict has been called 'the most socially mediated civil conflict in history' (Lynch, Freelon & Aday, 2014). This important use of cyberspace as an instrument of war is not addressed effectively under the provisions of IHL.

The introduction of cyber capabilities does not change the principles of IHL, which continue to require actions qualifying as attacks for the principles to apply. The mischief that can be caused with cyber-created disruption of civilian transportation and communication systems, while still falling below destructive activity, illustrates how time-honoured IHL principles fail to provide complete protection for civilians during armed conflict.

This limitation in international law is brought into stark focus in *Tallinn Manual 2.0*, rule 92, which defines cyber-attack as 'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to people, or damage or destruction to objects'. There are certainly times when destructive cyber operations would be a desired goal, especially operations conducted by terrorists, who may not have the requisite infrastructure and support system to carry out extended operations. To date, most cyber operations have not aimed to destroy or damage systems, however, because that type of effect can betray ongoing operations and end pathways into systems used for intelligence gathering and extended disruptive operations. Because of the secrecy surrounding cyber operations, there are few reported cases, but the ones that are reported have largely caused virtual rather than physical harm. And, when the effect is virtual, application of the law becomes much more difficult. Targeting civilians or civilian property with attacks, whether virtual or physical, expected to cause death, injury or property destruction is a violation of the IHL principle of distinction. On the other hand, disruption or interference alone does not meet the threshold of an attack, and even a cyber operation with these effects were to be targeted at civilians it would not violate the principle of distinction. This result reflects a serious limitation in the protection of civilians from the effects of cyber operations afforded by IHL.

The realization that IHL provides only limited protection for the civilian population from nonviolent cyber activity during war has led some scholars to suggest a redefinition of the concept of 'attack' in the cyber context to include, not just damage or destruction, but also a loss of system functionality. Such a reinterpretation of attack is impractical because it could encompass events such as blockading roads or shutting down civilian phone service temporarily, i.e., interfering with the functionality of the road or telephone. Expanding the definition of attack to such a degree would negatively affect the application of IHL to traditional warfare. Unless states decide to negotiate an expansion of the principles of IHL, or determine new customary law through practice, these suggestions will remain the musing of scholars.

Information and influence operations

Cyberspace capabilities have made it possible to spread information on a scale and at a speed that was simply not possible pre-Internet. Journalists, civilian groups, and corporations have all made use of this new capability, often in productive ways. Unfortunately, the new capabilities have also opened the possibility for states to ‘participate’ in the internal affairs of other states more effectively. This involvement has raised concerns, particularly in the case of elections.

One critical question is whether cyber-based attempts to manipulate elections violate international law. The obligation of states to hold ‘genuine periodic elections’ is enshrined in Article 25 of the *International Covenant on Civil and Political Rights* (ICCPR, 1966). That provision was designed to ensure states hold elections, not to preclude interference with the elections of other states. Interfering with external elections would violate the spirit of the ICCPR, but the agreement does not directly prohibit the activity.

Lacking more specific legal guidance, the relevant standard to determine if election interference activities are unlawful is whether the activity is a violation of sovereignty, perhaps a violation of the non-interference principle. (TM 2.0, Rule 66). In the case *Military and Paramilitary Activities in and against Nicaragua Case* (*Nicaragua v. United States of America*), the International Court of Justice noted that the principle of non-intervention involves ‘the right of every sovereign State to conduct its affairs without outside interference’. The ICJ concluded the prohibition on interference is part of customary international law, which forbids states from ‘interven[ing] directly or indirectly in internal or external affairs of other States’.

Unfortunately, the ICJ did little to clarify exactly what kinds of activities would constitute wrongful interference. Scholars have weighed in on the issue, and generally there is a consensus that attempting to manipulate an election would violate the nonintervention norm (Damrosch, 1989, pp. 1–50). How cyber enabled operations fit into that framework is still uncertain. This is another area of international law that will likely develop only with state practice.

International human rights law

Certain rights are recognized for all humans by treaty and by custom, and those rights exist in cyberspace as well as in physical space. At the most basic level, Article 3 of the *Universal Declaration of Human Rights* notes that ‘[e]veryone has the right to life, liberty and security of person’. The UN High Commission for Human Rights noted that human rights are equally valid online. (UNHCR, 2012). Article 19 of the Universal Declaration of Human Rights includes protections of freedom of speech, communication and access to information. In 2013, the UN General Assembly voted to confirm people’s ‘right to privacy in the digital age’ (UNGA, 2013).

Many human rights considered to be fundamental, such as self-determination and privacy, are protected in cyberspace in the form of protected speech and the right to private communications. The *Tallinn Manual* experts concluded that the right to freedom of expression, freedom of opinion, and freedom from arbitrary interference with privacy are customary international human rights laws, but also noted that the parameters of the protections of these rights in cyberspace are not yet clear. (TM 2.0, Rule 35)

The question of how to handle metadata is a specific human rights law issue. Metadata is information about data, including data necessary for delivery of emails and other Internet packets. Internet service providers must be able to view metadata for the proper functioning

and maintenance of the Internet. Governments may look to metadata to help monitor communications for the security of the state with a minimum of violation of individual privacy. However, metadata may also be analyzed to disclose much more information about individuals than is readily apparent. (Su et al., 2017) For now, metadata is largely unprotected, but there may be some privacy coverage for metadata under international human rights law yet to be articulated.

A UN Special Rapporteur suggested that access to the Internet is a human right, although his report did not state it explicitly. ‘Given that the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States’ (UN, 2011). It seems reasonable to conclude that if something is an *indispensable* tool for accessing a human right, the tool itself must be part of the right. This does not seem to be the majority opinion, at least not yet. The *Tallinn Manual* concludes that ‘technology is an enabler of rights, not a right as such’. (Rule 35, para 22) Vint Cerf, one of the ‘fathers of the internet’ holds a similar view. He noted, ‘technology is an enabler of rights, not a right itself. There is a high bar for something to be considered a human right. Loosely put, it must be among the things we as humans need in order to lead healthy, meaningful lives, like freedom from torture or freedom of conscience. It is a mistake to place any particular technology in this exalted category’ (Cerf, 2012).

Although access to the Internet is not itself a human right, it seems likely that as the importance of the Internet and cyberspace continue to increase, the recognition of rights associated with cyberspace will also grow. What the ultimate extent of those rights will be, and how they will be protected, remains to be determined.

Norms

Cognizant of the gaps in international law, especially with regard to civilian protections from the negative effects of cyberspace operations, several efforts to develop norms of appropriate state behaviour have been undertaken. Progress has been painfully slow, but the efforts have had some effect. One of the issues is that there is a disconnect among different efforts over exactly what international norms are. Without delving too deeply into the minutiae of the norms definition debate, suffice it to say most of the norms conversation seems to be centred around a desire to develop a non-binding involuntary code of conduct that is something more than empty declarations but less than law. It is perhaps true that the inability to agree on exactly what a norm is has led to an inability to agree on what norms should apply to cyberspace activities.

Leading the effort in the norms arena is the UN Group of Governmental Experts on cyberspace, officially the ‘Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (GGE). The efforts of that group seemed to be bearing fruit with reports that reflected an understanding of how an increasing number of international law principles apply to activities in cyberspace. In 2013, the third cyber GGE recognized that international law, and in particular the UN Charter, applies in cyberspace. That GGE also recognized the application of sovereignty and related principles to state cyberspace activities (UNGA, 2013).

The 2015 UN GGE on cyber went further in specifying lists of positive and limiting norms applicable to state cyber activities, including prohibitions on targeting other states’ cyber emergency response teams and intentionally damaging critical infrastructure (UNGA, 2015). However, the group was unable to accomplish more in the area of norms when the 2017 effort ended without producing a consensus report.

Leaving aside government-led efforts to develop norms, there has been some success on the private side. Several corporate-driven efforts have produced interesting products. States appear to have recognized the value of corporate contributions, and are using corporate efforts to boost state progress. Because corporations are so deeply involved in the operations of cyberspace, and indeed own much of the underlying infrastructure of the Internet, it seems appropriate that they would be involved in developing the rules of the road. More importantly, corporations are in a position to enforce general rules, as they have the ability to develop and run the infrastructure in a way that encourages compliance with the standards that are set.

An early private effort in this area was Microsoft's proposal for a Digital Geneva Convention. (Microsoft, 2017). That proposal would commit states to refrain from attacking critical infrastructure, refrain from hacking journalists' and electoral data, refrain from stealing intellectual property, and prohibit installing back doors in commercial technical products, among other things. Other corporate-led efforts include the Siemens *Charter of Trust* and Carnegie Endowment *Norm against Manipulating Financial Data*. While none of these lists of norms has been universally accepted, they serve to open the discussion between corporations and governments about the future of cyberspace, and may encourage appropriate corporate practices and government efforts that could coalesce into binding rules.

Another group is the Global Commission on the Stability of Cyberspace (GCSC), a joint effort between governments and corporate actors. Its early focus is on safeguarding what it refers to as the public core of the Internet, although it also seeks to protect elections and product development from cyber interference.

At this point none of the norms efforts is clearly leading the race to develop broadly followed and useful rules of the road for cyberspace. Even the discussion about appropriate state behaviour is valuable, however, so the conversation should continue. There can be no development of rules or agreement on norms without discussion, and cyberspace has been plagued with secrecy veiled the activities of states and prevented meaningful discussion about law and rules applicable in cyberspace.

Conclusion

An explosion is an explosion and a bullet is a bullet, but a data packet is not an airplane and inconvenience is not an injury. These contrasts may sound self-evident, but interpreting the existing system of international law so that it could govern cyber operations appropriately, protecting civilians and regulating the conduct of armed conflict, such equivalencies would be required. Applying law developed for kinetic operations to cyberspace activities is not a simple undertaking. To avoid the risk of stretching the application of international law beyond the breaking point, states must provide clarity through disclosed cyber practice and official statements.

It is likely states will continue to struggle to make political decisions on what constitutes a projection of force in cyberspace, and how to respond to cyber actions to which they fall victim. States may wish to maintain options for their own cyber forces, while also establishing enforceable rules to maintain international order. These two goals are not always compatible, but the current ambiguity leaves open the possibility of unintended escalation of international tensions.

Competition in cyberspace is inevitable, but conflict is not. However, in cyberspace offense trumps defence, so a framework for state operations is especially important. States require cooperation and understanding of the acceptable parameters for actions and responses

or chaos may become the norm. With most state operations being clandestine and unacknowledged, state practice has done little to provide clarity and predictability. What is required is an exercise of political will from leading states to develop a grammar of cyber actions, escalation, and response that will help avoid unintended conflict.

References

- Cerf, V.G. (2012) Access is not a human right. *New York Times* (4 January). Available from: www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html [accessed 7 June 2019].
- Coram, R. (2002) *Boyd: The Fighter Pilot Who Changed the Art of War*. New York, Little, Brown and Company.
- Damrosch, L.F. (1989) Politics across borders: Non-intervention and nonforcible influence over domestic affairs. *American Journal of International Law*. 83.
- Global Commission on the Stability of Cyberspace*. Available from: <https://cyberstability.org/> [accessed 7 June 2019].
- Holland, S. & Chiacu, D. (2014) Obama says Sony hack not an act of war. *Reuters* (20 December). Available from: www.reuters.com/article/us-sony-cybersecurity-usa-idUSKBN0JX1MH20141221 [accessed 7 June 2019].
- Holloway, M. (2015) Stuxnet worm attack on Iranian nuclear facilities. Available from: <http://large.stanford.edu/courses/2015/ph241/holloway1/> [accessed 7 June 2019].
- Human Rights Watch (2018) *Heed the Call: A Moral and Legal Imperative to Ban Killer Robots*. Available from: www.hrw.org/report/2018/08/21/heed-call/moral-and-legal-imperative-ban-killer-robots [accessed 7 June 2019].
- International Law Commission (ILC) (2001) *Draft Articles on Responsibility of States for Internationally Wrongful Acts*. Available from: http://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf [accessed 7 June 2019].
- International Committee of the Red Cross (ICRC) (2019) *Fundamental Principles of IHL*. Available from: <https://casebook.icrc.org/glossary/fundamental-principles-ihl> [accessed 7 June 2019].
- International Court of Justice (ICJ) (1986) *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*. I.C.J. Reports. Available from: www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf [accessed 13 June 2019].
- International Covenant on Civil and Political Rights (ICCPR)* (1966). Available from: <http://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf> [accessed 7 June 2019].
- Jennings, R. & Watts, A. (eds) (1992) *Oppenheim's International Law*, 9th edn. Oxford, Oxford University Press.
- Kellogg-Briand Pact* (1928). Available from: http://avalon.law.yale.edu/20th_century/kbpact.asp [accessed 7 June 2019].
- Lynch, M., Freelon, D., & Aday, S. (2014) Syria's socially mediated civil war. *US Institute of Peace*. Available from: www.usip.org/sites/default/files/PW91-Syrias%20Socially%20Mediated%20Civil%20War.pdf [accessed 7 June 2019].
- Microsoft (2017) *Digital Geneva Convention to Protect Cyberspace*. Available from: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH> [accessed 7 June 2019].
- Office of the Director of National Intelligence (ODNI) (2019) Global threats: Cyber. In *Worldwide Threat Assessment of the US Intelligence Community* (29 January). Available from: www.dni.gov/files/ODNI/documents/2019-ATA-SFR-SSCI.pdf [accessed 7 June 2019].
- Press, M. (2018) Of robots and rules: Autonomous weapon systems in the law of armed conflict. *Georgetown Journal of International Law*. 48. Available from: www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-4-Of-Robots-and-Rules.pdf [accessed 7 June 2019].
- Su, J., Shukla, A., Goel, S., & Narayann, A. (2017) De-anonymizing web browsing data with social networks. Available from: <http://randomwalker.info/publications/browsing-history-deanonymization.pdf> [accessed 7 June 2019].
- Richwine, L. (2014) Cyber attack could cost Sony studio as much as \$100 million. *Reuters* (9 December). Available from: www.reuters.com/article/us-sony-cybersecurity-costs/cyber-attack-could-cost-sony-studio-as-much-as-100-million-idUSKBN0JN2L020141209 [accessed 7 June 2019].

- Sanger, D. (2012) Obama order sped up wave of cyberattacks against Iran. *The New York Times* (1 June). Available from: www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [accessed 15 June 2019].
- Schmitt, Michael N. (ed.) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (TM)*. Cambridge, Cambridge University Press.
- Spamhaus (2017) *Spamhaus Botnet Threat Report*. Available from: www.deteque.com/app/uploads/2019/02/Spamhaus-Botnet-Threat-Report-2019.pdf [accessed 7 June 2019].
- Tikk, E, Kaska, K. & Vihul, L. (2010) *International Cyber Incidents*. CCDECOE, Tallinn.
- United Nations General Assembly (UNGA) (1974) Definition of Aggression. Resolution 3314 (XXIX) (14 December).
- United Nations General Assembly (2013) (UNGA) The Right to Privacy in the Digital Age. Resolution 68/167 (18 December).
- United Nations High Commission for Human Rights (2012) *Promotion and Protection of all Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development*. A/HRC/20/L.13 (29 June).
- United Nations (2011) *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. Frank La Rue, rapporteur. A/HRC/17/27 (16 May).
- United Nations General Assembly (UNGA) (2013) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/68/98 (24 June).
- United Nations General Assembly (UNGA) (2015) *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174 (22 July).
- White, S. (2018) Understanding cyberwarfare: Lessons from the Russia-Georgia war. Available from: <https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf> [accessed 15 June 2019].
- Wright, J. (2018) Cyber and International Law in the 21st Century. UK Attorney General speech, (23 May). Available from: www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [accessed 7 June 2019].

EXPLORING THE GENERAL PRINCIPLES OF INTERNATIONAL LAW IN THE CYBERSECURITY CONTEXT

Nohyoung Park and Myung-Hyun Chung

One of the most significant developments on how to regulate cyberspace must be the recommendation of the third Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) in 2013 that international law, and in particular the Charter of the United Nations (UN), is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible, and peaceful information and communications technologies (ICT) environment. Since then, the applicability of international law, including the UN Charter, to cyberspace, has been generally recognized internationally. The fourth UN GGE in 2015 rather successfully considered how international law applies to the use of ICTs, i.e. cyberspace, by states. However, the right to self-defence and international humanitarian law were roughly in an indirect way stated due to conflicting positions among the members of the UN GGE. The fifth UN GGE in 2017, however, failed to adopt a consensus report mainly due to the disagreement on how international law applies to the use of ICTs by states. The fourth UN GGE previously recognized the need for further study on the right to self-defence in particular. The explicit mentioning the latter and international humanitarian law in particular again became sources of the disagreement among the member of the fifth UN GGE. Although there are strong voices among a certain number of states for a new international agreement applicable to cyberspace, it may take more time until the international agreement for a need of such an international agreement is made. In the meantime, there is a good need to explore the general principles of international law to effectively work for cybersecurity. For this purpose, there is a good precedent: ‘Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations’ (Resolution 26/25 (XXV) (hereinafter, ‘1970 International Law Principles Declaration’) adopted during a commemorative session to celebrate the twenty-fifth anniversary of the UN on 24 October 1970 (UNGA, 1970).

The 1970 International Law Principles Declaration was adopted rather generally for friendly relations and co-operation among states some 50 years ago when cyberspace and the Internet were not even envisioned. However, the lessons from the study and adoption of the 1970 International Law Principles Declaration on how to procedurally and what to

substantially study and adopt might be useful to a similar declaration, to be adopted by the General Assembly, for cybersecurity.

The procedural history of the adoption of the 1970 International Law Principles Declaration

The process of agenda setting for the 1970 International Law Principles Declaration

On 18 December 1961, on the recommendation of the Sixth Committee, the General Assembly decided to place the item entitled 'Consideration of principles of international law concerning friendly relations and co-operation among States in accordance with the Charter of the United Nations' on the provisional agenda of its seventeenth session. The question was put forward by twelve delegations in the same year.

On 18 December 1962, the General Assembly at its seventeenth session, following the discussion of the question in the Sixth Committee, recognized the paramount importance, in the progressive development of international law and in the promotion of the rule of law among nations, of seven principles of international law concerning friendly relations and co-operation among states (UNGA, 1962: resolution 1815 (XVII)). Thus it resolved to undertake a study of the seven principles with a view to their progressive development and codification, so as to secure their more effective application. Those seven principles are:

- i) the principle that States 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;
- ii) the principle that States shall settle their international disputes by peaceful means in such a manner that international peace and security and justice are not endangered;
- iii) the duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the UN Charter;
- iv) the duty of States to co-operate with one another in accordance with the UN Charter;
- v) the principle of equal rights and self-determination of peoples;
- vi) the principle of sovereign equality of States; and
- vii) the principle that States shall fulfil in good faith the obligations assumed by them in accordance with the UN Charter.

(UNGA, 1962)

It decided accordingly to place the same item on the provisional agenda of its eighteenth session in order to study four of those seven principles and to decide what other principles were to be given further consideration at subsequent sessions and the order of their priority. Those four principles are the prohibition of the use of force, the peaceful settlement of disputes, the prohibition of intervention, and the sovereign equality.

On 16 December 1963, the General Assembly requested the Special Committee to include in its deliberations a study relating to impartial methods of fact-finding in relation to peaceful settlement of disputes (UNGA, 1963b: resolution 1967 (XVIII)). According to the General Assembly, the feasibility and desirability of establishing a special international body for fact-finding or of entrusting an existing organization with fact-finding responsibilities complementary to existing arrangements and without prejudice to the right of parties to any dispute to seek other peaceful means of settlement of their own choice was to be studied.

However, the 1970 International Law Principles Declaration did not cover the methods of fact-finding in relation to peaceful settlement of disputes.

The establishment of the Special Committee

On 16 December 1963, the General Assembly at its eighteenth session decided to establish a Special Committee on Principles of International Law concerning Friendly Relations and Co-operation among States (hereinafter 'Special Committee') (UNGA, 1963a: Resolution 1966 (XVIII)). The Special Committee would be composed of Member States to be appointed by the President of the General Assembly, taking into consideration the principle of equitable geographical representation and the necessity that the principal legal systems of the world should be represented. The President of the General Assembly appointed twenty-seven Member States to serve on the Special Committee (A/5689). It would draw up a report containing, for the purpose of the progressive development and codification of the four principles chosen by the General Assembly so as to secure their more effective application, the conclusions of its study and its recommendations. It was to take into account in particular: a) the practice of the UN and of States in the application of the principles established in the UN Charter; b) the comments submitted by Governments on this subject in accordance with resolution 1815 (XVII); and c) the views and suggestions advanced by the representatives of Member States during the seventeenth and eighteenth sessions of the General Assembly. Importantly, the governments of the Member States designated members of the Special Committee were recommended to appoint jurists as their representatives on the Special Committee in view of the general importance and the technical aspect of the item. The Secretary-General was requested to co-operate with the Special Committee, and to provide all the services and facilities necessary for its meetings, including: a) a systematic summary of the comments, statements, proposals and suggestions of Member States on this item; b) a systematic summary of the practice of the United Nations and of views expressed in the United Nations by Member States in respect of the four principles; and c) such other material as he deems relevant (UNGA, 1963a).

The Special Committee had thus functions to perform similar to those of the International Law Commission with respect to the codification and progressive development of international law. These functions also came expressly within the competence of the General Assembly under Article 13 of the UN Charter (UN, 1945). However, the task of the Special Committee differed from that of the International Law Commission, in that the latter traditionally prepared draft articles for ultimate adoption by States, whereas the former was set up to study certain principles and present a report capable of adoption by the General Assembly (UNGA, 1964: A/5746).

The activities of the Special Committee

From 27 August to 2 October 1964, for five weeks, the Special Committee met in Mexico City, and held 43 meetings in the course of its first session. The report of the Special Committee (UNGA, 1964: A/5746) was considered by the General Assembly in the framework of the Sixth Committee, at its twentieth session in 1965.

On 28 August 1964, the Special Committee at its second meeting agreed to give early consideration to the establishment of a Drafting Committee (A/AC.119/4). On 8 September 1964, the Special Committee at its fifteenth meeting agreed to decide to establish a Drafting Committee composed of fourteen members (A/AC.119/5). When the discussion of a subject

has been completed, the Drafting Committee should consider the proposals, amendments and records of the Special Committee. The Drafting Committee, on each principle and on the question of fact-finding, should have the task of preparing, without voting: 1) a draft text formulating the points of consensus; and 2) a list itemizing the various proposals and views on which there is no consensus but for which there is support. On 10 September 1964, the following representatives of the Special Committee's fourteen members joined the Drafting Committee: Argentina, Australia, Burma, Czechoslovakia, France, Ghana, Italy, Lebanon, Mexico, Nigeria, the USSR, the UK, the US, and Yugoslavia (A/5746).

On 20 December 1965, the General Assembly, after taking note of the report, decided to reconstitute the Special Committee to complete consideration and elaboration of the seven principles (UNGA, 1965: Resolution 2103 (XX)). It also requested the Special Committee to submit a comprehensive report on the results of its study of the seven principles in order for the General Assembly at the twenty-first session to adopt a declaration containing an enunciation of these principles.

From 1966 to 1969, the Special Committee met on annual basis in New York or Geneva and submitted reports (A/6230, A/6799, A/7326 and A/7619) to the General Assembly. At the twenty-fourth session in 1969, the General Assembly took a number of decisions relating to the celebration of the twenty-fifth anniversary of the UN, and, on 31 October 1969, it invited the Special Committee to expedite its work with a view to facilitating the adoption of an appropriate document by the General Assembly during a commemorative session to be held the following year (UNGA, 1969: resolution 2499 A (XXIV)). The General Assembly asked the Special Committee to submit a comprehensive report at the General Assembly's twenty-fifth session in 1970 (UNGA, 1969b, Resolution 2533 (XXIV)).

During the 1970 session, informal consultations, coordinated by the Chairman of the Special Committee, were held in Geneva. The basis for the consultations was the draft prepared by the Drafting Committee as adopted by the Special Committee in 1969 (A/7619). On 1 May 1970, the Special Committee adopted the report of the Drafting Committee (A/AC.125/L.86). The Special Committee heard the positions of the Governments on its work and added these statements to the draft 1970 International Law Principles Declaration (A/8018).

The draft 1970 International Law Principles Declaration was considered by the General Assembly at its twenty-fifth session in 1970. After the Sixth Committee considered it, 64 States sponsored a draft resolution for the 1970 International Law Principles Declaration. On 28 September 1970, the draft resolution was adopted without objection by the Sixth Committee (A/8082). On 24 October 1970, the General Assembly adopted, without a vote, resolution 2625 (XXV), where the 1970 International Law Principles Declaration was approved in an annex (UNGA, 1970).

The implications for adopting an International Law Principles Declaration in cybersecurity context

From the experiences of the UN General Assembly and the Special Committee in particular for studying and adopting the 1970 International Law Principles Declaration, a process to study and adopt an international law principles declaration in cybersecurity context might be thought of. First, the General Assembly should initiate this important work. In accordance with Article 10 of the UN Charter, the General Assembly may discuss any questions or any matters within the scope of the UN Charter, and, in accordance with Article 13(1) (a) of the UN Charter, it shall initiate studies and make recommendations for the purpose of

promoting international cooperation in the political field and encouraging the progressive development of international law and its codification. It is to be noted that the General Assembly is obliged to 'initiate studies and make recommendations' to promote international cooperation in the political field and encourage the progressive development of international law and its codification (UN, 1945). The UN GGEs have been working for more than 15 years, but their achievements in applying international law to cyberspace in particular have run out of power due to conflicting and uncompromising positions among members, including the five permanent members of the Security Council. Cybersecurity, a non-existing concept and concern when the UN Charter was drafted, is certainly becoming the most important concern for international peace and security as well as for international economy and human rights. Thus, it is the right time for the General Assembly to tackle its task given in the UN Charter.

One of the reasons for the failure of the fifth UN GGE (2016–2017) to deliver a consensus report may be a diplomatic and political approach among 'the governmental experts'. Sometimes at least some of them appeared not to have a good knowledge of international law in discussing how international law applies to cyberspace. The Special Committee the UNGA established in 1965 was, however, fortunately composed of jurists, as recommended by the General Assembly, 'in view of the general importance and the technical aspect of the item', i.e., securing more effective application of international law. There were well-known international lawyers at that time in the Special Committee, including Mr. Hans Blix from Sweden, serving as rapporteur for the Special Committee, Mr. Taslim Olawale Elias from Nigeria, Sir Ian McTaggart Sinclair from the UK, and Mr. Stephen Myron Schwebel from the US. Thus, a special committee, to be established for studying and adopting an international law principles declaration in cybersecurity context, should consist of international lawyers with a good understanding of ICTs or cyberspace.

The Special Committee worked for a net period of six years after its establishment until submitting a draft 1970 International Law Principles Declaration. Thus, it would take a rather long period of years for such a special committee to achieve its tasks even after the agreement made in the UN General Assembly to initiate a study on an international law principles declaration in cybersecurity context. Another problem with this task may be an increasingly faster development of ICTs which would not wait for international lawyers to cope with them. In this respect, a group of experts in ICTs should be invited to give an independent and objective opinion and advice for those members of a special committee.

General principles of international law to be agreed in cybersecurity context

A need to find general principles of international law in cybersecurity context

An international law principles declaration in cybersecurity context, which may be similar to the 1970 International Law Principles Declaration adopted by the General Assembly on 24 October 1970, is worthwhile to study and adopt for the friendly relations and co-operation among States for cybersecurity. The principles of the UN Charter, embodied in the 1970 International Law Principles Declaration, were declared to constitute basic principles of international law (UNGA, 1970, Resolution 2625 (XXV)). A main reason for adopting such a declaration in a form of a resolution of the General Assembly is that the UN Charter was adopted so many years earlier before the creation of the Internet and

cyberspace and their useful and malicious uses have been seriously noted internationally. Strictly speaking, the UN Charter does not have any explicit or implicit references to cyberspace and the Internet.

The General Assembly (1964) has recognized that the UN Charter was incomplete in certain respects, and could be supplemented by the adoption of declarations codifying and developing certain UN Charter provisions. Such declarations include the Universal Declaration of Human Rights of 10 December 1948 (Resolution 217A), the Declaration on the Granting of Independence to Colonial Countries and Peoples of 14 December 1960 (Resolution 1514 (XV)), and the Declaration on the Elimination of All Forms of Racial Discrimination of 20 November 1963 (resolution 1904 (XVIII)). These Declarations were adopted without votes. They are regarded to be of great practical importance and have become, through general acceptance, part of the common law of mankind (UNGA, 1964, A/5746).

It is to be noted that declarations could be a useful method of making progress towards the development of new international law in certain new areas, where Member States wish to break new ground. A good example is the Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space, adopted by the General Assembly in December 1963 (UNGA, 1963, Resolution 1962 (XVIII)).

The four principles of international law to be agreed in cybersecurity context

The following four principles are cornerstones of peaceful relations among states:

- i) the principle that States 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;
- ii) the principle that States shall settle their international disputes by peaceful means in such a manner that international peace and security and justice are not endangered;
- iii) the duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the UN Charter;
- iv) and the principle of sovereign equality of States.

(UNGA, 1964)

These four principles of international law, far from being subordinate branches of international law, are binding all States as general principles of law (UNGA, 1964: A/5746). Likewise, as the 2015 UN GGE report notes, in their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States (UNGA, 2015). It is to be noted that existing obligations under international law are applicable to State use of ICTs. In considering the application of international law to state use of ICTs, as a matter of fact, the fourth UN GGE identified as of central importance the commitments of states to the following principles of the UN Charter and other international law: sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining 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 UN; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other states (UNGA, 2013).

Prohibition of the use of force

It is the first principle of the 1970 International Law Principles Declaration that States 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. Likewise, a cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the UN is unlawful (Schmitt, 2017, Rule 68, p. 329). Article 2(4) of the UN Charter provides that all Members 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 UN. The prohibition of the use of force is certainly a norm of customary international law (ICJ (1984), paras. 188–190).

There are two exceptions to the prohibition on the use of force – uses of force authorized by the Security Council under Chapter VII and self-defence pursuant to Article 51 of the UN Charter and customary international law. According to *Tallinn Manual 2.0* 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 (Schmitt, 2017, Rule 69, p. 330). A cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force (Schmitt, 2017, Rule 70, p. 338). The term cyber operation may be defined as ‘the employment of cyber capabilities to achieve objectives in or through cyberspace’ (Schmitt, 2017, p. 564).

Peaceful settlement of disputes

It is the second principle of the 1970 International Law Principles Declaration that states shall settle their international disputes by peaceful means in such a manner that international peace and security and justice are not endangered. Likewise, again according to *Tallinn Manual 2.0*, states must attempt to settle their international disputes involving cyber activities that endanger international peace and security by peaceful means (Schmitt, 2017, Rule 65(a), p. 303). Article 2(3) of the UN Charter provides that all Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered. Article 33(1) of the UN Charter also provides that the parties to any dispute, the continuance of which is likely to endanger the maintenance of international peace and security, shall, first of all, seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice.

If states attempt to settle international disputes involving cyber activities that do not endanger international peace and security, they must do so by peaceful means (Schmitt, 2017: Rule 65(b), p. 303). Article 2(3) of the UN Charter provides that all Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered. The term cyber activity may be defined as ‘any activity that involves the use of cyber infrastructure or employs cyber means to affect the operation of such infrastructure’. Such activities include cyber operations (Schmitt, 2017: p. 564).

Although the General Assembly requested the Special Committee to include it its deliberations a study relating to impartial methods of fact-finding in relation to peaceful settlement of disputes, the 1970 International Law Principles Declaration does not cover this matter. Interestingly, some twenty years later, in December 1991, the General Assembly, by

resolution 46/59, adopted, without a vote, the Declaration on Fact-finding by the United Nations in the Field of the Maintenance of International Peace and Security, the text of which was annexed to the resolution. It sets out principles for the acquisition of detailed knowledge by the UN about the factual circumstances of any dispute or situation that might threaten the maintenance of international peace and security (UNGA, 1991). The principles on fact-finding in the Declaration may be further developed for cybersecurity purposes, e.g. in the objective and transparent attribution of malicious cyber operations to States under the law of international responsibility.

Prohibition of intervention

It is the third principle of the 1970 International Law Principles Declaration that a state has the duty not to intervene in matters within the domestic jurisdiction of any state, in accordance with the UN Charter. Likewise, a state may not intervene, including by cyber means, in the internal or external affairs of another state (Schmitt, 2017, Rule 66, p. 312). This principle is based on the international law principle of sovereignty, specifically that aspect of the principle providing the sovereign equality of states (Schmitt, 2017, Rule 66, para.1, p. 312). Thus, a state is prohibited to do coercive intervention into the internal or external affairs of another through cyber means (Schmitt, 2017, Rule 66, para.1, p. 312).

Sovereign equality of states

It is the sixth principle of the 1970 International Law Principles Declaration that all States shall enjoy sovereign equality. Likewise, the principle of state sovereignty applies in cyberspace, as sovereignty is a foundational principle of international law (Schmitt, 2017, Rule 1, p. 11). Various aspects of cyberspace and State cyber operations are not beyond the reach of the principle of sovereignty (UNGA, 2013, para. 20; UNGA, 2015, para. 27). A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it (Schmitt, 2017, Rule 3, p. 16). This external sovereignty derives from the sovereign equality of states (Schmitt, 2017: Rule 3, para. 1, p. 16).

Article 2(1) of the UN Charter provides that the UN is based on the principle of the sovereign equality of all its members. Thus, in accordance with the UN Charter, the basic importance of sovereign equality is reaffirmed and the purposes of the UN can be implemented only if states enjoy sovereign equality and comply fully with the requirements of this principle in their international relations (UNGA, 1970, Resolution 2625 (XXV)). External sovereignty covers the freedom to formulate foreign policy (ICJ, 1984: para. 205), including to enter into international agreements (PCIJ, 1923: p. 25). Such sovereignty is the source of state immunity.

Conclusion

Since the third UN GGE recommended the applicability of international law, including the UN Charter, to the use of ICTs by States, i.e., cyberspace in 2013, the task for the UN and its Member States has been to agree to how international law really applies to cyberspace. While the non-governmental experts of international law were successful in publishing the *Tallinn Manual* twice in 2013 and 2017, the governmental experts of the UN Member States were not successful in agreeing to how international law applies to cyberspace in 2017. Although it may be a tough task to apply international law in general to cyberspace, it may be

rather an easier and concrete task to apply the UN Charter in particular to cyberspace. The UN Charter must be a primary collection of international law principles applying especially for international peace and security.

A so-called international law principles declaration in the cybersecurity context may be worthwhile to study and adopt for the friendly relations and co-operation among states for cybersecurity, following the 1970 International Law Principles Declaration adopted by the General Assembly on 24 October 1970. A main reason for adopting such a declaration in a form of a resolution of the General Assembly is that the UN Charter was adopted so many years earlier before the creation of the Internet and cyberspace and their useful and malicious uses have been seriously noted internationally. Simply speaking, the Internet and cyberspace are not reflected in the UN Charter. Thus, it may be necessary to examine the UN Charter in cybersecurity context, as it has been internationally agreed that the UN Charter is applicable to cyberspace since 2013.

If such a declaration of international law principles in cybersecurity context is to be studied and adopted, then the experiences of the UN General Assembly and the Special Committee for the 1970 International Law Principles Declaration are to be carefully studied as a good precedent. One of the successful achievements of the Special Committee may be its composition. Jurists were recommended by the General Assembly to work as members of the Special Committee.

Although those international law principles covered in the 1970 International Law Principles Declaration had been studied and adopted before the Internet and cyberspace were created and found, they must in principle apply to the latter. The Member States of the UN have recognized the applicability of international law, including the UN Charter, to cyberspace, and the *Tallinn Manual* has also convincingly indicated that international law could really apply to cyberspace.

It is, however, true that resolutions of the General Assembly do not in themselves constitute international law. As the most important element in the process of evolving international law is universality, such resolutions should reflect consensus so as to be capable of unanimous adoption by the General Assembly. Overall, a declaration of general principles of international law in cybersecurity context should be more than a mere reiteration of the provisions of the UN Charter and should take into account the evolution that have occurred in international law since the drafting of the UN Charter both in the practice of states and of the UN. The provisions of various multilateral treaties and of certain declarations of major international significance in peace and security, economy and human rights, which are related to ICTs, the Internet and cyberspace, should be taken account of. Further, concrete texts of such principles should secure their more effective application by states. As the 1970 International Law Principles Declaration was adopted during a commemorative session to celebrate the twenty-fifth anniversary of the UN, it is hoped that a declaration of general principles of international law in cybersecurity context may be adopted during such a session to celebrate the eightieth anniversary of the UN in 2025.

References

- International Court of Justice (ICJ) (1984) Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Judgement (26 November).
Permanent Court of International Justice (PCIJ) (1923) Case of the S.S. *Wimbledon* (United Kingdom, France, Italy & Japan v. Germany). Judgment (17 August).
Schmitt, M.N. (ed.) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press.

- United Nations (UN) (1945) *Charter of the United Nations*.
- United Nations General Assembly (UNGA) (1961) Future Work in the Field of the Codification and Progressive Development of International Law. Resolution 1686 (XVI) (18 December).
- United Nations General Assembly (UNGA) (1962) Consideration of Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations. Resolution 1815 (XVII) (18 December).
- United Nations General Assembly (UNGA) (1963a) Consideration of Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations. Resolution 1966 (XVIII) (16 December).
- United Nations General Assembly (UNGA) (1963b) Question of Methods Fact-Findings. Resolution 1967 (XVIII) (16 December).
- United Nations General Assembly (UNGA) (1964) Consideration of Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations. Report of the Special Committee on Principles of International Law concerning Friendly Relations and Co-operation among States. A/5746 (16 November).
- United Nations General Assembly (UNGA) (1965) Consideration of Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations. Resolution 2103(XX)A-B (20 December).
- United Nations General Assembly (UNGA) (1969a) Celebration of the twenty-fifth Anniversary of the United Nations. Resolution 2499 A (XXIV) (31 October).
- United Nations General Assembly (UNGA) (1969b) Consideration of Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations. Resolution 2533 (XXIV) (8 December).
- United Nations General Assembly (UNGA) (1970) Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations. Resolution 2625 (XXV) (24 October).
- United Nations General Assembly (UNGA) (1991) Declaration on Fact-finding by the United Nations in the Field of the Maintenance of International Peace and Security. Resolution A/46/59 (9 December).
- United Nations General Assembly (UNGA) (2013) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/68/98 (24 June).
- United Nations General Assembly (UNGA) (2015) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174 (22 July).

WHAT DO WE TALK ABOUT WHEN WE TALK ABOUT INTERNATIONAL CYBERSECURITY

Eneken Tikk

In the central question of the Handbook – what do we talk about when we talk about international cybersecurity – lies not just curiosity about the focus and scope of the conversation. Therein lies a conclusion that the international dialogue on international cybersecurity will only intensify in the coming years, and a conviction that governments and corporations must take their rights and responsibility to participate in this conversation seriously.

This chapter addresses five critical questions from the Handbook: What is international cybersecurity about? What acute peace and security threats are embedded in the use of ICTs? What trends and tendencies in state behavior are of potential concern to the international community? Which issues pertaining to the use of ICTs could be framed as ‘international issues of cybersecurity’ due to their frequency, scope or intensity? Do the current dialogues adequately address the concerns of the international community?

What is international cybersecurity about?

The authors of this volume have identified ICTs as a keen object of political dramatization (Dunn Cavelty, Chapter 1; Salminen and Kerttunen, Chapter 7), and a surface and tool of contemporary conflict (Mitchell and Pytlak, Chapter 2), but also as an object of everyday information security practices (Dunn Cavelty, Chapter 1), governance (Lan, Chapter 6), development (Krutskikh and Streltsov, Chapter 22), and a platform for human rights and freedoms (Purdon and Vera, Chapter 19).

Dunn-Cavelty’s (Chapter 1) observation that cybersecurity politics occupies a continuum between securitization and technological routine, depending on the context and sub-issue under scrutiny, brings to mind a US view from two decades ago. Pushing back on the Russian proposition of ICTs as a threat to international peace and security, in its 1999 submission to the UN First Committee the US maintained:

Although the general topic includes aspects that relate to international peace and security, it also includes technical aspects that relate to global communications, as well as

non-technical issues associated with economic cooperation and trade, intellectual property rights, law enforcement, anti-terrorist cooperation and other issues.

(United States of America, 1999, p. 11)

Two decades later, nobody contests the breadth of the issue. Lan (Chapter 6) notes that, having become pivotal to international security, economic development, trade, the environment and human rights, the Internet now penetrates most traditional public policy issues.

Readers will find the cybersecurity analysis cutting and pasting into established disciplines of computer science, international relations and international law. Without independent object or methods, fuelled by political ambitions, this quasi-discipline trends towards Virilio's (2000, p. 3) *extreme science*, exiling other disciplines from their reason. Maennel's (2019) thoughts help illustrate the composition of cybersecurity: from computer science it takes secure software design, or understanding how to build intrusion detection systems as well as methods for vulnerability testing; cryptography is rooted in mathematics; psychology helps to understand human factors; aspects of forensic science are used by law enforcement agencies; social sciences, business and economic understanding are essential to the design and marketing IT products and services; operational and strategic risk management models and audits help with reducing the threats in day-to-day operations; legal and political disciplines offer frameworks for directing broader societal trends and addressing unwanted consequences. This analysis leads Maennel to conclude that *cybersecurity* has become simply an expression for interdisciplinary attention to the development and use of ICTs. Dunn Cavelty seconds this, noting that military analogies like 'cyberweapons', 'cyberoffence', and 'cyberdefence', are just different words for well-known computer tools and information assurance concepts (Chapter 1).

Returning to the ground disciplines and applying a 'cyber-less' lens to the discourse, we can learn that securitization of the uses of ICTs is promoted and exploited by a rather narrow contingency of states and non-state actors (Dunn Cavelty, Chapter 1), that cyber diplomacy is, after all, simply 'diplomacy' (Feakin and Weaver, Chapter 24), and that cyber conflict is really about conflict.

The purpose of *cybersecurity*, however clear, is contingent – to draw attention to the neglected considerations of safety and security of products and services that have come to underpin how things are done and life is lived, and to manage the overlooked, and increasingly conflicting, security needs. Whilst experts avoid the word, politicians love it for the ambiguity it provides.

What acute peace and security threats are embedded in the use of ICTs?

A stock-taking of the peace and security-worthiness of ICTs indicates that most of international cybersecurity issues are not acute international peace and security concerns. Even in the military domain, cybersecurity practices are predominantly about technical, normal, and routine practices like mitigating risks to information networks by technical (and occasionally organizational) means (Dunn Cavelty, Chapter 1; UNIDIR, 2013). Despite the rhetoric towards developing military cyber capabilities, only a few NATO countries have moved towards an actual operational capacity of military cyber force (Pernik, Chapter 14). In this context, Mitchell's and Pytlak's findings about the predominantly dyadic and low-effect nature of cyber conflict support earlier findings by Valeriano and Maness (2019) and deserve to be scrutinized in national decision-making. Defending against cyber conflict may not be equally likely or relevant to all states, and without due analysis of one's situation, defending

against non-existent or abstract threats may nullify the expected benefits of the ICTs in the first place.

Furthermore, Kerttunen's analysis (Chapter 12) challenges the immediate threat and impact of cyberterrorism. Kerttunen clarifies that there is clear evidence of terrorist groups making increasingly advanced use of digital systems and services. However, little points to their attempts or appetite towards destroying information and industrial systems by digital means. He makes another compelling argument against adding cyberterrorism among the focal points of the UN First Committee. Noting that problematizing cyberterrorism as a serious, real problem, nationally or internationally, will remain subject to the very different criteria applied to define terrorism, he also makes reference to a near-universal, pre-existing solution to where terrorist aspirations in the context of the use of ICTs would become a concern of international peace and security. The United Nations Security Council (UNSC) Resolution 1373 (2001), Kerttunen reminds us, qualifies 'any act of international terrorism' as a threat to international peace and security.

What trends and tendencies in state behavior are of potential concern to the international community?

Although generally not conflict-grade, the use of ICTs for political purposes has become an alarming reality that requires response from any and all states. Cynical use of ICTs for political purposes has become an alarming reality. In line with Mitchell and Pytlak, Demchak regards the appetite and skill of 'aggressive acquisition of foreknowledge' as particularly a precursor to further, potentially more intense and aggressive cyber posturing (Chapter 3). In this context, it is equally paramount to pay attention to emerging state practices and the emerging tolerance for cyber operations flagged by Mitchell and Pytlak (Chapter 2), Krutskikh and Streltsov (Chapter 22). Demchak (Chapter 3) concludes that cyber conflict, even though characterized by limited actors and low effects, constitutes a 'continuing source of uncertainty and insecurity for all states'. With reference to Mallery, she notes that this conflict will be particularly hard for states that intend to survive as consolidated democracies.

Further concerns for international peace, security and stability are flagged in the Handbook. As Tikk and Kerttunen (Chapter 4) note, new entrants have come onto the scene of international conflict and contestation. Pernik (Chapter 14) further notes that creating cyber commands has become partially an opportunistic tendency with unclear effects and consequences. Salminen and Kerttunen (Chapter 7) conclude that cyber militancy results in an increased ability and willingness to project national power in and through cyberspace, paired with decreased attention to the foundations of sustainable peace and stability. This, they argue, diminishes the authority of law, produces inequality, affects the protection of human rights and fundamental freedoms, and inhibits development. Libicki (Chapter 10) warns that cyber-capable states' behaviour largely hinges on self-restraint – their contingent lack of motivation to trash commercial, industrial or governmental systems and networks given the perceived advantages of cyberespionage. These inhibitions, Libicki maintains, are not guaranteed in a crisis or conflict.

The list of potential issues does not end here. Lewis (Chapter 21) notes that the US is moving beyond debates on 'whether an US retaliatory act would violate the sovereignty of the nations whose networks it traveled, and whether it was necessary to first ask the permission of those nations before acting'. Moving on from 'the Obama administration's legalism' Lewis admits, 'involves the risk of escalation of conflict, in cyberspace and elsewhere'. In the US view, this probability can be managed through diplomatic action and by a calculus of

proportionality and an opponent's appetite for risk. This, however, flags the concerns raised by Tikk and Schia in their analysis of the role of the UN Security Council (Chapter 30) – adherence to the rule of law is an indispensable element for the prevention of armed conflict.

In sum, it is clear that the intersection between international peace and security and the use of ICTs should not be dismissed. It remains unclear what, exactly, is the problem and the prospects involved.

Which further issues pertaining to the use of ICTs could be framed as ‘international issues of cybersecurity’ due to their frequency, scope or intensity?

If the notion of *international* in international cybersecurity is not a mere reference to peace and security, the dialogue must be understood as a much more fundamental one. Several authors propose a different focus and direction for international cybersecurity – the internationalization of issues pertaining to the development and certain uses of ICTs. For instance, Martin (Chapter 8) notes that without a balanced and detailed account on all causes of insecurity, threats to security become ‘naturalized’, treated as inevitable. What, then, are the true issues of international cybersecurity – those that have come to concern a substantive number of states so that it merits international dialogue and agreement? What issues have become global and require universal approaches? Which are best suited for regional coordination and what can be taken up on a bilateral basis?

Contreras and Barrett (Chapter 16) usefully ask how to provide a vehicle to ensure the positive impact ICTs can have on economic growth, competitiveness, prosperity and security of the humankind. Ang (Chapter 17) offers another useful question for any decision-maker to consider: Why does a country need to spend its resources on regional (here, ASEAN) and international cybersecurity efforts? For Singapore, the answers and evidence of action are insurmountable, as evidenced by Lim and Sok's account on developments in ASEAN and CLMV (Chapter 18). Their hope that the story of the CLMV experience may shape international cyber and information security negotiations towards more sustainable concept of peace, stability, and development, is inspiring.

Tropina (Chapter 11) observes that the past two decades have witnessed a steady growth of cybercrime. Whether this means that there is more criminal activity now or that states and organizations have just got better at detecting and counting individual crimes is not clear. Tropina agrees that cybercrime threatens international economic integrity and is likely to target citizens of even the most advanced information societies (Levy, 2018). Despite cybercrime being an acute issue for states, and calls for harmonized legal standards to criminalize certain acts and provide investigation tools as the key in tackling cybercrime (Goodman, 2010; Sieber, 2008), Tropina is left to conclude that the hope for a global and universal solution is slim, to a large extent due to the resistance of the countries party to the Council of Europe Cybercrime treaty, also known as the Budapest Convention. Attempts to make the Budapest arrangement a global solution have not succeeded, either. Here, Russia has been clear about the Council of Europe solution being out of its comfort zone.

In addition, Purdon and Vera (Chapter 19) warn that a predominant focus on combating cybercrime may leave *actual* cybersecurity, essentially a technical approach to securing systems such as critical infrastructure and consumer services from attack and failure, largely under-resourced. They note that both in Africa and the Americas, states have criminalized what could be considered the legitimate exercise of human rights protected by human rights instruments. Further to this discussion, Seger (2019) says that over-securitization leads to

systemic violations of rights and freedoms, including freedom of information, due process and privacy. He points out that most cyber incidents would justify and require investigation as crime or other breaches of law but are, in fact, now followed up by such investigations or procedures – they are either reduced to technical incidents and resolved as such, or elevated to political/national security issues and then addressed in these terms. Investigations move from criminal justice procedures, to national security arena which does not help with human rights and rule of law in cyberspace. Seger concludes that without effective measures to prevent and prosecute cybercrime, we accept a massive violation of rights. All nations claim interference in elections, but nobody has instigated criminal proceedings, no confidence in criminal justice. Cybercrime violates rights, like privacy, democracy, and Pytlak (Chapter 5) makes the daunting conclusion that the question of human rights is largely overlooked in multilateral discussions of cybersecurity. Her findings, supported by Sander (2017) are aggravated by the analysis of PoKempner (2017)

Others raise further leads for international discussions. Demchak (Chapter 3) concludes that cybered conflict's central pursuit is the aggressive acquisition of access to accurate and current data. Butrimas (Chapter 9), with reference to Schneier, emphasizes that electronic espionage can become an active breaking into an adversary's computer network, likely to be accompanied by installing malicious software on that network, which he considers an action violating the sovereignty of another country. Demchak (Chapter 3) also underscores that clandestine intrusions into networks are made possible by 'shoddy creation of the current cyberspace'. Indeed, the ratio of penetration of networks and theft of data among reports of cyber incidents testify if a severe lack of resilience.

Butrimas (Chapter 9) points out alarming trends in the behavior of some states and state-sponsored groups. Attacks against safety systems and control mechanisms, he notes, are beyond what IT cybersecurity specialists were trained for. The question, however, does not only become one of defence. Martin (Chapter 8) proposes that more focus is required on removing or reducing the cyber threats, rather than defending against them. In this context, another of Dunn Cavelty's observations is worth repeating. She concludes that actual cybersecurity practices are often about technical, unexceptional practices like mitigating risks to information networks by technical (and occasionally organizational) means (Chapter 1).

Do the current policies adequately address the concerns of the international community?

According to Lewis (Chapter 21), US policy is slowly coming to 'recognize the world as it is' – conflictive and dominated by states, and not as it was imagined when the United States was unchallenged. This, Lewis argues, 'makes conflict more likely than peace'. With this Melian argument, Lewis meets Butrimas (Chapter 9), who suggests that the lack of an international security mechanism only contributes to furthering this destabilizing behaviour that risks much wider and more dangerous conflict.

The shift towards normalizing the use of cyber weapons is observed by Krutskikh and Streltsov (Chapter 22). US Deputy Assistant Secretary of State Strayer's (2019) remarks also confirm Butrimas's point about 'legitimizing' the use of cyber weapons: 'As cyber capabilities become cheaper and easier to acquire, more States are establishing offensive cyber programs. States must use these capabilities responsibly.'

This makes confidence building (Meyer, Chapter 25) timely and relevant between established and aspiring cyber powers. However, as Hovhannisyan (2019) observes, what the UN GGE has framed as CBMs do not really fit the original blueprint of reducing tension

and unpredictability. Publicly known cyber incidents involving cyber powers are not accidental, they are intentional. Kerttunen and Salminen (Chapter 7) posit that voluntarism, embedded in the norms approach to international cybersecurity, is hardly a guarantee for responsible behaviour. Instead of 'planting statist, corruptive and antagonist frameworks on the use of ICTs and advanced technologies', Salminen and Kerttunen call for more granular attention to the behaviour of states and the issues causing conflictual behaviour and focus on promoting trust, cooperation, societal development, and individual welfare and empowerment.

Amazouz (Chapter 15) suggests that the work done so far at international and regional levels in developing norms, rules and confidence building measures to prevent escalation, misperceptions, and conflicts in cyber domain may not have served the actual concerns of the global community (Chapter 15). Lim and Sok, analysing the situation in the CLMV countries, conclude that issues that many states face, such as financing, legal and administrative frameworks, infrastructure, work force competence and an overall domestic culture of cybersecurity, cannot be achieved by focussing on strategic stability between the cyber superpowers or debates on *jus in bello*. Chernenko, Demidov and Lukyanov (2018) challenge international cybersecurity's preoccupation with massive state-sponsored attacks and devastating casualties. Consequently, they ask about the relevance and consequences of the expert work done in the UN First Committee over the past two decades.

As a way ahead, Krutskikh and Streltsov see ICT penetration, and the resulting spread of issues, as a reason to broaden the scope, as well as the membership, of the international dialogue (Chapter 22). From his part, Lewis puts a definitive full stop to the illusions of multi-stakeholder political system, 'where civil society and corporations would be equal partners to governments'.

Conclusion

ICTs have become a pawn in a game of high political ambitions. Cyberspace cannot be more or less secure than 'real' spaces. Discussions of territory, ownership, jurisdiction, and control flow from the conceptualizing cyberspace as yet another space. However, acute cybersecurity issues cannot, and should not, be isolated from broader strategy and security questions – if the world is getting more conflictual, so will the cyberspace.

The time to talk about international cybersecurity is now. This talk needs to be realistic, concrete, and self-critical. Martin (Chapter 8) underlines governments' unique position in directing research, investment and implementation related to cyber vulnerabilities. However, can governments, in their hypersecuritizing aspirations, be trusted to invite and support good research? Purdon and Vera (Chapter 19) throw down a gauntlet to governments, questioning the legitimacy of developing cybersecurity policy and legislation without appropriate analysis of the risks, threats, and beneficiaries of their agendas. In particular, they point out how combatting cybercrime has become a way for governments to exercise control over online activities.

Moving ahead, an array of cybersecurity issues is to be discussed and allocated to respective responsibilities at the international, national, organizational, and individual level. Can the 'plastic' still be turned, as Lessig (2006) suggests? ICTs alone neither make nor prohibit any state from becoming militant, Salminen and Kerttunen (Chapter 7) conclude, retelling Lessig's (2006, p. 32) point that technology can be made to reflect any set of values. To get to a positive change is becoming more and more challenging without decisive new voices, cooperation, and a meaningful proposition for a 'third way'.

Without clear ideas and visions about how to steer the international dialogue, we must be prepared to see cybersecurity turning into an environmental problem. With the amount of media attention, academic programmes, and publications dedicated to it, savings from printer pages turn into trees spent on booklets, newspapers, national strategies, and airport literature. However, in this sea of opinions and stands, little points to any international solution. Flying thousands of cyber experts and government representatives to endless meetings to repeat their positions, control the political temperature and occasionally encounter the private sector and civil society, ‘in their respective roles’, produces hot air and carbon dioxide rather than securing the exciting and innovative ways ICTs can support peace and development, and societal and individual empowerment.

References

- Chernenko, E., Demidov, O. & Lukyanov, F. (2018) Increasing international cooperation in cybersecurity and adapting cyber norms. Available from: <https://eng.globalaffairs.ru/book/Increasing-International-Cooperation-in-Cybersecurity-and-Adapting-Cyber-Norms-19391> [accessed 17 September 2019].
- Goodman, M. (2010) International dimensions of cybercrime. In Ghosh, S. & Turrini, E. (eds) *Cybercrimes: A Multidisciplinary Analysis*. Berlin and Heidelberg, Springer-Verlag.
- Hovhannissyan, K. (2019) *Confidence-Building Measures and Cyber Conflict Prevention*. Tallinn, Tallinn University of Technology
- Lessig, L. (2006) *Code: Version 2.0*. New York, Basic Books.
- Levy, I. (2018). *Active Cyber Defence – One Year On*. United Kingdom National Cyber Security Centre Available from: <https://www.ncsc.gov.uk/blog--post/active-cyber-defence-one-year> [accessed 17 September 2019].
- Maennel, O. (2019) <https://www.maennel.net/> [accessed 17 September 2019].
- Maness, R.C., Valeriano, B. & Jensen, B. (2019) The dyadic cyber incident and dispute data, Versions 1, 1.1, and 1.5. Available from: <https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset> [accessed 17 September 2019].
- PoKempner, D. (2017) Squinting through the pinhole: A dim view of human rights from Tallinn 2.0. *Texas Law Review*. 95(7): 1599–1617.
- Sander, B. (2017) 13(e). In Tikk, E. (ed.) *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary*. New York, UN Office for Disarmament Affairs. pp. 95168.
- Seger, A. (2019) Interview.
- Sieber, U. (2008) Mastering complexity in the global cyberspace: The harmonization of computer-related criminal law. In Delmas-Marty, M., et al. (eds) *Les chemins de l'Harmonization Pénale/ Harmonising Criminal Law, Collection de L'UMR de Droit Comparé de Paris*. Paris, Société de législation comparée, pp. 127–202.
- Strayer, R.L. (2019) Remarks at a Joint U.S.–Mexico Reception at the OAS for Participants of the UN GGE Regional Consultation. Available from: www.state.gov/remarks-of-deputy-assistant-secretary-robert-l-strayer-at-a-joint-u-s-mexico-reception-at-the-oas-for-participants-of-the-un-gge-regional-consultation/ [accessed 17 September 2019].
- United Nations Security Council (2001) Resolution 1373.
- United States of America (1999) Submission to the Developments in the Field of Information and Telecommunications in the Context of International Security. UN Document A-54–213.
- Virilio, P. (2000) *The Information Bomb*. London and New York, Verso.

Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

INDEX

Note: Bold page numbers refer to tables

- advanced persistent threat (APT) 124, 141–144, 187, 219, 252
- adversary 25, 39, 42, 54, 149, 175–176, 180–183, 190, 224, 367
- African Union 83, 151, 157, 205, 206–207, 235–236, 246
- Arab Spring 55, 66, 297–299, 301
- Arab states 81, 116, 151, 205
- armed attack 264, 312, 368–372
- armed conflict 41, 100, 170, 181, 186, 240, 257, 264, 287–291, 355–356, 366–373, 376, 392
- armed forces 4, 57–58, 96, 98–102, 137, 175, 181, 186–195, 219, 289, 359, 368–370
- ARPANET 328–329
- artificial intelligence (AI) 39, 81–86, 94, 183, 186, 271, 283, 321, 360
- ASEAN Regional Forum (ARF) 203, 207, 224, 228, 266, 294, 335, 344, 392
- assistance 60, 152–157, 203–207, 225, 228, 235, 239–242, 249–250, 266–267, 278, 313, 316
- Association of Southeast Asian Nations (ASEAN) 83, 151, 205, 206, 218–225, 227–232, 280–282
- attribution 24, 32, 57, 97, 127–146, 150, 170, 253, 256–257, 262–264, 282, 290, 358–360, 386
- awareness 39, 74, 80, 101, 142–143, 148, 151–157, 175, 188–195, 201–208, 215–216, 220, 225, 228–230, 249–250, 269, 288, 301, 332–333, 366
- bilateral 6, 27–32, 52–61, 156, 166–170, 201, 216, 219, 242, 349, 392
- Bitcoin 123, 320
- blockchain 86, 320, 349
- botnet 40, 156, 369
- BRICS (Brazil, Russia, India, China, South Africa) 82–84, 163
- Budapest Convention 82, 151–157, 205, 236–237, 242–243, 248–249, 392
- capability 23–25, 32, 37, 42, 54–58, 94–103, 117, 127, 149, 167–170, 176, 186–195, 202–206, 224, 228, 249–250, 253–255, 266–271, 280–282, 288–289, 294–295, 299–303, 308, 331–333
- capacity building 57, 61–61, 69, 88, 145, 151, 201–210, 215–217, 219–221, 224–225, 227–229, 232, 239–243, 250, 254, 265, 278–280, 282–283, 303, 334–335
- censorship 45, 67–68, 169, 238, 360
- Central Intelligence Agency (CIA) 117
- Christchurch 168, 317, 321–322
- cloud 81, 139, 270, 313, 220, 257, 358
- CLOUD Act 156–157, 317
- code of conduct 55, 201, 289, 375; and international code of conduct 318, 322
- colour revolution 55, 66
- Comprehensive Study on Cybercrime 153–155
- computer emergency response team (CERT) 137, 204, 220–224, 228–231, 240, 270, 291, 326, 331, 375
- computer network operations 99, 327, 332
- computer security incident response team (CSIRT) 191, 207, 229–231, 327–329, 332–336
- confidence-building measures (CBM) 1, 4, 6, 60, 69, 82–83, 91, 101–103, 126–128, 151–153, 202–203, 208–210, 221, 225, 240–249,

- 254, 266, 280–282, 286–295, 303, 319, 333, 393–394
- cooperation 2, 4; bilateral 52, 56; cross-border 148, 156, 343–345; cybercrime 82–84, 150–151, 154–157, 205, 277, 282; economic 52, 151, 335, 390; intelligence 137, 192; multi-stakeholder 149, 156, 167, 203, 223, 267; and regional 91, 151, 155–156, 189, 206–207, 214–217, 219, 223–225, 227–243, 247–250, 266
- countermeasures 7, 15–18, 61, 79, 97, 101–102, 135, 139–142, 145–146, 165, 169, 179, 257, 271–372; collective 102, 262
- Crimea 174, 181–182, 356
- critical infrastructure 14, 43, 56, 58, 95, 122–131, 161–165, 169, 178, 186, 190–193, 209, 214–215, 221, 231, 235, 250, 263, 280–282, 289, 291, 294, 304, 315–318, 323, 348, 357–358, 361–362, 375–376, 392
- cryptography 137, 347, 390
- cyber conflict 22–33, 36–47, 57, 70, 74, 363, 366–371, 390–391
- cyber command 42, 100–101, 188–195, 255, 391
- cyber crime 15, 82, 148–157, 163, 207, 224, 227–230, 235, 239, 241, 253, 270, 319, 371, 393
- cyber operations 5, 6, 24–25, 32, 61, 72–75, 83–85, 97, 100–103, 174, 177–178, 187–191, 194–195, 201, 208, 252–253, 256–257, 281–282, 286, 291, 294, 304, 315–318, 323, 348, 357–358, 361–362, 375–376, 392
- cybersecurity strategy 203, 205, 209, 215, 218–219, 240–241, 250, 269
- Cyber Security Technology Agreement 84
- cyber threat 97, 111, 126, 149–150, 161, 190–194, 201, 204–207, 214–217, 219, 230, 249, 320, 329, 344, 356, 363, 393
- cyberterrorism 5, 97, 161–170, 270, 391
- cyber war 36, 97–98, 126, 183, 305, 318, 257
- cyber warfare 98, 101, 175, 289, 295, 366–367
- cyber weapon 16, 24, 75, 98, 122–127, 131, 298, 304–305, 308, 318, 323, 393
- data breach 218–219, 234
- data protection 80, 84, 87, 101, 157, 206, 225, 229, 236, 243, 248
- defensive 1, 12, 25, 32, 101, 127–129, 146, 186–187, 190–191, 204, 252, 271, 306–307, 312, 314, 323, 373
- democratic processes 312, 315–316, 361
- denial-of-service attack (DOS)/distributed denial-of-service (DDoS) 15, 125, 135, 143, 164, 224, 230, 329, 348–349, 257, 373
- Department of Commerce 81, 302
- Department of Defense 80, 94, 138, 188
- Department of Homeland Security (DHS) 253
- Department of Justice 255
- Department of State 57, 70, 101, 206–207, 349
- deterrence 4, 6–7, 23–25, 53–55, 75, 83, 98, 101, 127–128, 150, 169, 181, 190, 255–258, 262
- development: economic 74, 80, 86, 221, 227, 241, 247, 262, 270, 390; societal 1, 4, 62, 102, 394; sustainable 3, 60–61, 170, 227, 260, 266, 277, 283–284, 289, 356; and technological 54, 81, 90, 100, 183, 195, 208
- digital divide 61, 81, 84, 225, 248, 260, 252–263, 266
- Digital Geneva Convention 73, 84, 128, 304, 318, 376
- digitalization 2, 55, 61, 94–98, 102, 214, 229–230
- disarmament 57, 68–72, 74–75, 90, 100, 120, 204, 220, 267, 288–289
- doctrine 3, 56, 84, 94, 99–100, 164, 174–180, 182–183, 188–189, 192–193, 195, 239, 255, 359
- domain name system (DNS) 59, 79, 84, 261
- dual-use 83, 98, 152, 166, 272, 297, 299–302, 305–308, 347
- Economic Community of West African States (ECOWAS) 207, 236, 247–250
- effects: denial 165, 187, 349; degradation 165, 168, 170, 187, 349; destruction 4, 14, 18, 41–43, 53, 55, 58–59, 114–115, **115**, 161–162, 164–165, 170, 254, 369, 370–371, 373; disruption 13, 37, 42, 52, 58, 112–119, 125, 148, 157, 165–169, 176, 187, 219, 223, 251, 349, 357, **358**, 367, 373; injury 165, 323–324, 372–373, 376; loss of life 4, 126, 131, 161–165, 170, 172–173, 194, 205–207, 217, 219, 224, 229–231, 234–238, 242–243, 248–250, 317, 329, 343, 394; and manipulation 165, 168, 176, 223, 271, 357, 361, 367, 373–374
- elections 168, 177, 179–180, 190, 235, 255, 262, 315–319, 356, 361, 369, 374, 376, 393
- electromagnetic 100, 111–112, 120, 164, 191
- electromagnetic pulse (EMP) 111–112, 120
- electronic warfare 97, 99–100, 191
- emerging technologies 6, 83, 94, 186
- encryption 73, 86, 96, 112, 114–115, **115**, 118, 241–242, 299, 342, 346–347
- Equifax 138–139
- escalation 4, 24–25, 32, 41, 54–57, 102–103, 125, 129, 195, 204–210, 240, 255–257, 291, 334, 359–363, 370–371, 376–377, 391, 394
- espionage 6, 23, 56, 61, 74, 96–97, 127–128, 135, 149, 188–190, 253, 315, 351, 357, 369, 393
- Estonia 2007 61, 164
- Eternal Blue 123, 136, 138
- European Union (EU) 39, 72, 83–85, 87, 117, 125, 151–156, 167, 179, 205, 234–235, 255, 301–302, 307, 317, 345, 347

- European Union Agency for Cybersecurity (previous name European Union Network and Information Security Agency) (ENISA) 129, 333
- export controls 166–167, 170, 297–309, 346–347
- extremist 67, 88, 163–164, 166, 168, 315, 317, 321–323
- Facebook 39, 59, 66, 88, 116–117, 164, 167–169, 236, 315–317, 319–321
- facial recognition 239, 299
- fake 59, 86, 114, 116, 168, 179, 266
- FIRST (Forum of Incident Response and Security Teams) 335
- Five Eyes 117, 137
- freedom of expression 2, 4, 27, 67–68, 71–73, 155, 235–238, 241, 282, 313–316, 360, 374
- freedom of information 84, 393
- Georgia 2008 61, 373
- Global Commission on the Stability of Cyberspace (GCSC) 72, 85, 202, 335, 376
- Global Cybersecurity Index 203, 220, 227, 248
- Google 39, 85, 88, 167, 303, 317, 321
- governance 1–2, 5–6, 17, 27, 40–47, 60–61, 71, 79–91, 202, 208, 229, 252–254, 261, 264, 269–271, 277, 312–317, 322–324, 327–330, 336, 356, 360, 364
- Great Firewall 56, 120
- hacking 5, 99, 142–143, 162–163, 243, 257, 298–299, 349, 376
- hidden functions 264, 357, **358**; services 179
- hostile 45, 47, 113, 119, 150, 253–257, 260–262, 290, 316, 370
- human rights 1–2, 5–6, 62, 66–75, 80, 85–86, 91, 104, 120, 152, 165–167, 169–170, 205–209, 225, 234–239, 241–243, 254, 262–265, 277–279, 282–283, 297–299, 302–303, 305–306, 308, 312–314, 322–324, 356–360, 367, 374–375, 383–387, 389–393
- human security 66, 312, 314–316, 318, 322–324, 356
- hybrid war/fare 36–47, 98, 359, 362
- ICT for Peace Foundation 167
- implementation: capacity building 204–208, 216–217, 250, 263; confidence-building measures 82, 203, 266, 286; export controls 278, 301–303, 306–308; human rights 66, 68, 237; norms and rules 60, 87, 90, 203, 221, 253, 304, 318, 323; policies and strategies 89, 189, 194, 209, 216, 240, 250, 266, 271, 278–280, 322, 334, 336; trade regulations 343–345, 348
- incident: management 170; response 205–207, 215–216, 228–231, 282, 291, 301–303, 326–329, 331–336, 342; *see also* CERT; CSIRT
- incidents 18, 26–27, 53, 57–62, 67, 80, 102–103, 125, 135–145, 164–165, 169–170, 201–209, 224, 231, 239, 253–255, 261–266, 270, 281–282, 290–291, 331–332, 334, 355, 357, 361–364, 393–394
- indictment 141, 255, 257
- industrial control system 123–125, 270, 358, 369, 371
- influence operation 168, 179, 374
- information: free flow of 2, 59, 85, 304; operations 55, 100, 174–183, 191, 193, 223, 257, 288–289; security 1–3, 7, 53–58, 69–73, 82, 97, 114, 164–170, 178–179, 193, 203, 231–232, 260–267, 270, 290, 329, 389–392; warfare 55, 97, 99–100, 174–175, 179, 182–183, 188, 289
- innovation 40, 43, 46, 59, 79, 81, 89, 91, 95, 148, 222, 225, 236, 272, 290, 305
- insecurity 6, 13, 18, 36, 46–47, 52, 61–62, 103, 117, 129, 166, 170, 315, 391–392
- instability 25, 32, 52, 54, 57, 60–61, 235, 290, 358
- intellectual property 39, 85, 88, 237, 282, 321, 343–345, 347, 370, 376, 390
- intelligence: agencies/community 12, 15–16, 111, 113, 120, 137, 144, 237, 240, 247, 299, 312, 316; capabilities 24, 97, 101, 194, 204; collection/gathering 38, 168, 312, 373; operations 39; signal (SIGINT) 38, 100
- International Court of Justice 370, 374
- international cybersecurity 3–5, 70–75, 201–202, 219–220, 232, 234, 314, 327, 332–333, 389–394
- international law: applicability 60, 66–74, 83, 88, 128, 150, 166, 202–203, 221, 225, 257, 260–261, 263, 279–280, 291, 301, 341–342, 366–376, 379, 383–384, 386–387; Commission 381; crisis of 262; customary 263, 370, 373–374, 385; development of 61, 126–128, 150, 201, 262–264, 336–337, 380–381, 383; existing 45, 57, 152–153, 280, 282; humanitarian law (IHL) 60, 69, 74, 150, 167, 264, 291, 302, 356, 366, 372, 379; human rights law (IHRL) 66, 68–70, 72, 74, 299, 367, 374–375; inconsistency with 3, 28; norms of 262, 264; principles 264–265, 379–387; public international law 101, 150
- international system 53, 178–179, 265, 269, 334
- International Telecommunication Union (ITU) 151, 177, 203, 208, 220, 227, 266
- Internet Corporation for Assigned Names and Numbers (ICANN) 79, 81–84, 89, 261, 263, 313–314, 328–329, 335
- Internet Engineering Task Force (IETF) 314, 328

- internet governance 2, 61, 71, 79–91, 202–208, 254, 264, 277, 320, 327–329, 336
- Internet Governance Forum (IGF) 202, 320, 328
- internet of things (IoT) 81, 88, 129, 138, 186, 215–218, 271, 283
- internet penetration 27, 29–31, 234, 247
- internet protocol 313; IP address 56, 313, 328, 330
- Internet Research Agency 190, 255
- internet shutdowns 67, 116–117; terrorist use 150, 161, 167–168, 362
- Interpol 83, 151
- Islamic State of Iraq and the Levant (ISIS) 167, 169
- joint military: operations 186, 255, 257; planning 3, 80, 100, 189
- jurisdiction 71, 82, 152, 154, 167, 209, 262–263, 313–316, 380–386, 394
- kill-chain 142
- killing 119, 370; *see also* effects: loss of life
- lethal autonomous weapons (LAW) 83, 367
- law enforcement 15, 94, 128–129, 137, 148–150, 156–157, 162, 168–170, 194, 202, 205–206, 237, 250, 282, 290, 297–299, 312, 317, 332–323, 390
- legal assistance 152, 154–157, 316
- legislation 68, 73, 86, 97, 149, 151–156, 168
- malicious: actors 149–150, 263, 281, 359; code/software 16, 100, 128, 215, 308, 393; cyber activities 57, 102, 122, 124, 128–131, 208, 253–257, 281–282, 346–348, 351, 369, 386; use of technologies 65, 69, 83, 164, 203, 291, 358
- malware 111, 122–125, 129–130, 140–143, 164, 215, 229, 231, 282, 300–308, 329, 349, 367–368, 372
- man-made 59, 81, 261
- Microsoft 73, 84, 123–124, 128, 136, 138, 167, 202, 215, 304, 317, 321
- militarization 15, 23, 33, 74, 94–104, 241, 334
- multilateral 65, 68, 75, 80–91, 154, 189, 201–205, 269, 286–291, 297–298, 304–306, 327, 344–345, 349, 387, 393
- multi-stakeholder 314, 324
- National Security Agency (NSA) 39, 101, 103, 113, 117–118
- Network: governance 79, 269–270; intelligence 127; operations 99; operator 139, 327–336; security 83, 87, 95, 100, 207, 269–272, 330, 332–333
- NotPetya 41, 123, 131, 135–136, 282, 361
- normative 4–5, 12, 14, 61, 67, 167, 170, 232, 341
- norms: development 33, 240, 313, 327, 336; norms, rules and principles 7, 60, 103, 127, 202, 225, 260–265, 291, 304; recommendations 69, 129, 224, 231, 254, 263–264, 280, 303–304, 323; (of) state behaviour 57, 82–84, 101, 134, 209–210, 221, 231, 253, 255, 280–281, 303–304, 367, 375
- North Atlantic Treaty Organization (NATO) 15, 82–83, 174, 176, 178, 180, 186–195, 286, 354, 390
- nuclear weapons 24–32, 53–55, 58, 65, 74–75, 103, 112, 123, 363
- offensive 1, 12, 15, 32, 42, 85, 100–103, 111, 127–128, 134, 137–146, 186–192, 204, 280–281, 288, 295, 304–305, 307, 312–318, 321, 342, 370, 373, 393
- operating system 123–124, 135, 136, 169, 297
- Organization for Security and Co-operation in Europe (OSCE) 82–83, 203, 240, 266, 286–287, 293, 294
- Organization of American States (OAS) 83, 151, 203, 205–206, 214–217, 239–243, 294, 335
- Paris Call 72, 202, 317, 339, 320–321
- peace and security 4–5, 52, 65, 68–69, 161–62, 165–166, 354–363, 385–386, 390–391
- peaceful cyberspace 72, 85, 209, 295, 327
- peaceful settlement 2, 104, 380–381, 385–386
- persistent engagement 101, 146, 255–258
- power: balance 53, 140, 252; cyber 24, 42–44, 98–102; military 22, 101–102, 164, 178–181, 189, 195, 252
- pre-emptive 13, 98, 190, 262
- prevention: conflict 53, 57, 103, 170, 190, 287, 290, 293–295, 350, 356, 363, 392; crime 82, 148, 153–155, 166, 237, 241, 277, 282, 332
- privacy 3, 39, 67–73, 80, 85, 114, 138–140, 150, 234–238, 241–242, 248, 315–316, 327, 344–346, 375–375, 393
- private sector 15, 43, 73–74, 79–80, 86–89, 95, 103, 128, 153–154, 209, 215–216, 222, 242, 249–250, 282–283, 290, 306, 312–324, 335, 347, 362, 364, 395
- propaganda 83, 117, 162–163, 174–182, 223, 281, 288
- proxy 38, 47, 293
- quantum computing 94, 186, 282
- ransomware 41, 123–124, 149, 219, 271, 282, 361
- reflexive control 181

- regional: approaches 225, 234–239, 240–243; cybersecurity 203–207, 215, 231, 234–243, 249; instruments 151, 155; organizations 151, 153, 155, 203, 214–215, 249, 286; security 3, 53, 91, 170, 221, 300, 316
- regime: change 45, 56; control 167, 237, 297; legal 2, 43, 55, 156, 264, 269, 299, 318, 341, 346, 349; system 44, 57, 58, 67, 116, 145, 179, 229, 252, 257, 297–298, 302, 305, 356, 361
- resilience 6, 37, 42–46, 54, 61, 103, 129, 138–140, 161–162, 169–170, 202–203, 209, 215, 225, 250, 252–253, 318–320, 327–336, 393
- resources 36–47; financial 42, 203, 227, 249; human 103, 209, 217, 227–230; information 55–56, 75; internet 79–80, 328–329
- response: collective 43, 46–47, 101, 188, 262; incident 215–216, 228–229, 282, 301, 303, 331–332, 336; international 82, 124, 126, 127, 209; law enforcement 148, 150, 153–154; military 46, 96, 98, 168; teams (*see* CERT; CSIRT)
- responsibility: accountability 14, 27–32, 201–202, 208, 281, 324; legal 262, 264, 386; private sector 84–85, 88; shared 91, 203, 209, 241, 249, 323, 331, 362, 389; state 6, 60, 66, 83, 130, 166, 201, 261, 300, 322, 356, 368–369, 371
- regulation (of) 86, 168, 179, 262, 279, 297–309, 341, 346
- retaliation 23–26, 32, 37, 40, 58, 127, 252–258
- retorsion 257, 371–372
- Revolution in Military Affairs (RMA) 175, 288
- risk management 59, 215, 253, 318, 364, 390
- rule of law 61, 104, 170, 205, 221, 252, 312, 356, 380, 392–393
- rules of engagement 57, 192, 312
- rules of the road 279–281, 376
- sabotage 23, 113–115, **115**, 119, 289, 357
- safeguards 148, 150, 152, 157, 235, 237, 243, 349
- safety instrumented system (SIS) 124–125, 127
- sanctions 83, 165, 257, 279, 342, 348–349, 368
- Saudi Aramco 41–42, 164
- securitization 11–19, 23, 95–99, 102, 179, 334, 389–390, 392–393
- SCADA (supervisory control and data acquisition) 124–125, 270
- Siemens 138
- Siemens Charter of Trust 84–85, 317–318, 324, 376
- smart 103, 167, 209, 215, 218–219, 225
- Snowden 61, 67, 80, 117–118, 119, 313
- social media 39, 66–67, 88, 114, 117, 164, 168–170, 175, 179, 223, 236, 257, 313, 315, 373
- sovereignty: cyberspace 56, 238, 270, 272, 361, 368; non-intervention/-interference 55, 386; state 2–3, 69–71, 81, 89, 153, 209, 225, 254–255, 261–263, 270, 314, 334, 356, 360, 368–369, 375, 384–386; violation of 128, 368–369, 374, 391, 393
- stability of cyberspace 5, 13, 53, 55–61, 72–73, 201, 204, 208, 261, 335
- Stuxnet 41, 61, 111, 122, 124, 127, 130, 138, 164, 371–372
- supply chain 41, 138, 216, 231, 271, 317–318, 324, 348, 357, **358**
- surveillance 2, 13, 56, 67–68, 73, 102, 113–120, 167–168, 194, 234–243, 297–308, 312–315, 330, 360
- Tallinn Manual* 83, 369–375, 385–387
- targeting 27–30, 41, 67, 112–113, 118, 123–130, 136, 144, 149, 165, 168, 214–215, 281, 299–300, 304, 307, 357, 373, 375
- Tech Against Terrorism 167
- threat to international peace and security 3, 161, 165, 167, 288, 302, 354–355, 357, 362, 389, 391
- threshold 14, 41, 102–103, 146, 195, 257, 359, 370–373
- Twitter 66, 88, 107–109, 321
- uncertainty 36, 46, 86, 90, 123, 152, 209, 222, 257–258, 289–290, 357, 370–371, 391
- unilateral 6, 83, 101, 148, 155–157, 255, 342
- United Nations (UN): Charter 4, 6, 61, 66, 69–70, 165, 261–263, 279, 355, 357, 363, 369–370, 375, 379–387; General Assembly (UNGA) 3, 55, 68–73, 82, 84, 129, 153–154, 201, 254–255, 260–267, 280, 287–292, 303–304, 326, 356–363, 370, 374, 380–387; Group of Governmental Experts (GGE) 6, 69–71, 82–84, 126–128, 161–163, 202, 208–209, 231–232, 240, 254, 280, 287–293, 303, 319, 322, 357, **358**, 361–363, 375, 379–386, 393; Institute for Disarmament Research (UNIDIR) 100, 204, 288–289, 335; Open-Ended Working Group (OEWG) 56, 70, 82, 260, 265–267, 292, 363; Secretary-General (UN S-G) 61, 68–69, 79, 91, 209, 221, 277, 287, 289, 357, 362–363, 381; Security Council (UNSC) 4–6, 52, 70, 73, 161, 165–167, 170, 254, 262, 280, 354–364, 383, 385, 391–392
- Universal Declaration of Human Rights 61, 66, 71, 334, 384
- use of force 1–2, 257, 262, 265, 359, 364, 368–372, 380, 384–385
- vendor 137–139, 190, 314, 318, 333
- victim 24, 41, 58, 127, 136, 165, 215, 218, 302, 368–369, 371–372, 376

Index

- violence 52–53, 67, 74, 113, 161, 164–170, 183, 223, 235, 321, 323, 359
- vulnerability 6, 13, 22–24, 28, 32, 54, 58, 61–62, 85, 96, 98, 111–120, 123–124, 135–145, 148, 162–170, 177–183, 186, 203–208, 214, 222, 230–231, 241, 247–250, 270, 291, 297, 301–303, 312, 318, 323–324, 329, 347, 351, 357–359, 357, 362, 390, 394
- WannaCry 41–42, 123–124, 136, 271, 282, 361
- war 2–6, 15–16, 23–33, 38–42, 47, 52–60, 100–102, 114–115, **115**, 131, 180–183, 355–364, 367–372; *see also* cyber war; cyber warfare; hybrid war/fare
- Wassenaar Agreement 83, 167, 269, 297–309, 347
- weapons of mass destruction 55, 74, 94, 170, 254
- World Summit on Information Society (WSIS) 79–80, 83, 91, 153, 202, 208, 261–262, 328
- World Trade Organization 38–39, 279, 343–346
- YouTube 66
- zero-day 137–139, 146, 297