Report

So Far, Yet So Close

Japanese and Estonian Cybersecurity Policy Perspectives and Cooperation

| Henry Rõigas and Tomas Jermalavičius (editors) |
| Jun Osawa | Kadri Kaska | Liis Rebane | Toomas Vaks |
| Anna-Maria Osula | Koichiro Komiyama |

May 2021

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI • ESTONIA

Title: So Far, Yet So Close: Japanese and Estonian Cybersecurity Policy Perspectives and Cooperation
Authors: Rõigas, Henry (editor); Jermalavičius, Tomas (editor); Osawa, Jun; Kaska, Kadri; Rebane, Liis; Vaks, Toomas; Osula, Anna-Maria; Komiyama, Koichiro
Publication date: May 2021
Category: Report

Cover page photo: The cherry blossom (桜, sakura), Japan's unofficial national flower, on the Harju Hill in Tallinn, with the Cross of Liberty of the Monument to the War of Independence (Vabadussõja võidusammas) on the Freedom Square visible behind. Tallinn, Estonia, May 2021, by ICDS.

Keywords: cooperation, cybersecurity, cyber diplomacy, cyber threat, international norms, strategy, Japan, Estonia

ISSN 2228-0529
ISBN 978-9916-9657-0-2 (print)
ISBN 978-9916-9657-1-9 (pdf)

63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee, www.icds.ee

Acknowledgements

We are very grateful to all friends and colleagues who greatly facilitated this project and thus enabled this report. We would like to thank Mari Tomingas and her colleagues at the Cyber Diplomacy Department of the Estonian Ministry of Foreign Affairs; Oliver Ait and Argo Kangro at the Estonian Embassy in Japan; Piret Urb from the Estonian Information Systems Authority (RIA) and Keiko Kono from the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn; Lauri Korts-Pärn and Cdr Ide Tatsuo, convenors of the CyDef conference in Tokyo; and Ambassador Hajime Kitaoka and his team at the Embassy of Japan in Tallinn.

About the authors

Tomas Jermalavičius

Tomas Jermalavičius is Head of Studies and Research Fellow at the International Centre for Defence and Security (ICDS). Prior to joining ICDS, he worked at the Baltic Defence College (BALTDEFCOL) in Tartu, Estonia, and Lithuanian Ministry of National Defence. Since 2017, he also has been a visiting professor at the Natolin Campus of the College of Europe in Warsaw. He holds a BA in political science from the University of Vilnius, an MA in war studies from King's College London and an MBA degree from the University of Liverpool.

Kadri Kaska

Kadri Kaska has been head of the Legal Branch and legal researcher of cybersecurity policy at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) since 2008. Her main area of research is national cybersecurity strategy and governance; as part of her portfolio, she maintains the Centre's National Cybersecurity Strategies repository and is editor of the "National Cybersecurity Governance" series. In 2017–18 she was seconded to the Estonian Information System Authority, where she was the lead author and editor of annual Estonian Cyber Security Assessments and contributed to the agency's activities in cyber threat assessment, policy analysis and legal drafting. In that capacity, she was one of the authors of Estonia's new Cyber Security Act and the 2018 Cyber Security Strategy. She holds a master's degree in law from the University of Tartu.

Koichiro Komiyama

Dr Koichiro Komiyama has been a visiting scholar at Keio University's Global Research Institute (KGRI) since 2016 and Director of the Global Coordination Division at the Coordination Centre of the Japanese Computer Emergency Response Team (JPCERT/CC), which he joined in 2007. Since 2017, he has also been Deputy Chair of the Research Advisory Group at the Global Commission on the Stability of Cyberspace (GCSC). In 2014–18, he served on the Board of Directors of FIRST (Forum of Incidents Response and Security Teams). He received his PhD from Keio University Graduate School of Media and Governance in 2020 and holds a BA in Business Administration from Aoyama Gakuin University.

Jun Osawa

Jun Osawa is Senior Research Fellow at Nakasone Peace Institute (NPI, formerly Institute for International Policy Studies, IIPS). He is also a board member of Kajima Peace Institute, Cyber Project Coordinator at Sasakawa Peace Foundation, Visiting Research Fellow at the Air Staff College, and serves on the staff of the National Security Secretariat (NSS). He joined NPI/IIPS in 1995 as a research fellow before becoming a senior research fellow in 2009. Some of his previous positions include: Senior Fellow and Deputy Cabinet Counsellor at the NSS; Visiting Fellow at the Brookings Institution; visiting scholar at the National Graduate Institute for Policy Studies, and Policy Planning Researcher and Advisor at the Policy Planning Division of the Ministry of Foreign Affairs. He holds a BA and an MA degrees from Keio University.

Anna-Maria Osula

Dr Anna-Maria Osula is a senior policy officer at the Estonian software security company Guardtime, with a focus on cybersecurity policy and regulation and supporting international R&D projects. She also serves as a senior researcher and lecturer at TalTech, and as a research fellow at Masaryk University in Czechia. She previously worked as a legal researcher at the NATO CCDCOE, focusing on national cybersecurity strategies, international organisations, and international criminal cooperation and norms. She is also the founder of an annual conference series "Interdisciplinary Cyber Research", which has been organised by TalTech since 2015. In addition to a PhD in law from the University of Tartu, she holds an LLM degree in IT law from Stockholm University.

Liis Rebane

Dr Liis Rebane is a cyber-risk professional, contributing to risk control in the field of cyber and ICT risks at the largest Estonian bank, Swedbank. Prior to focusing on challenges in the financial sector since 2018, she served as the head of Estonian Cyber Security Policy in the Ministry of Economic Affairs and Communications, guiding the design, follow-up, and stakeholder management of the National Cyber Security Strategy. She holds a PhD degree in physics from the University of Tartu.

Henry Rõigas

Henry Rõigas is a Non-Resident Research Fellow at ICDS and Chief Strategy Officer at Sentinel. Previously, he was the Head of Research and Innovation Cooperation at the cyber security company Guardtime and a member of the Board of Directors at the International Association for Trusted Blockchain Applications (INATBA). Before joining Guardtime, he published analysis and managed international projects at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) as a policy researcher. While at the CCDCOE, he was the Agenda Director for CyCon, the world's leading cyber defence conference. He holds an MA in International Relations from the University of Tartu.

Toomas Vaks

Toomas Vaks is a cyber-risk manager at Swedbank Group. He joined this company in 2000 and held various positions in the fields of risk management, fraud investigations, corporate security, KYC and AML/CTF compliance, and served as head of Risk Management in Group Cards. In 2011, he moved to the government sector and became Deputy Director General of the Information System Authority (RIA), where he founded and headed the Cyber Security Branch, responsible for the development of the National Cyber Security Strategy and incident response planning, state-level crisis and incident management and coordination, security operations and other functions. In 2017, he rejoined Swedbank Group. He holds an MA degree in social sciences from Tallinn University of Technology (TalTech).

Executive Summary

Given the differences in their physical attributes, such as location and size of territory and population, as well as in their historical development trajectories and their cultures, Estonia and Japan appear very dissimilar. At the same time, they have many significant commonalities, rooted in a strong commitment to underlying democratic values, shared concerns about the future of liberal international order and comparable challenges to their national security. As highlighted in the four chapters of this report, authored by leading cybersecurity experts and practitioners from the two countries, there are also shared factors that flow from the complex cybersecurity challenges faced by both countries. Cybersecurity is an important area where Japan's and Estonia's concerns, interests and approaches converge and where advancing their bilateral cooperation is an important undertaking. With the aim of facilitating this cooperation through the exchange of national best practices and experience, this research report is devoted to sharing perspectives on Japan's and Estonia's cybersecurity policy.

The first chapter is written by Jun Osawa, Senior Research Fellow at Nakasone Peace Institute, who provides an overview of the cyber threat landscape, highlighting the different types of cyber operations that are actively undertaken by nation-states. Although the chapter describes the situation from the Japanese perspective, it is evident that the challenges described and the possible responses to them are relevant to many like-minded states, such as Estonia. The chapter describes several strategies that can be undertaken to deter the ongoing malicious behaviour of states in cyberspace. First, the author advocates that nations should continue to develop a comprehensive approach to cyber deterrence that utilises principles of Active Cyber Defence – meaning that nations should develop capabilities and strategies that not only focus on building effective defensive measures, but also allow for proactive responses against sophisticated attacks by adversaries. These can be in the form of cyber counterattacks or other international policy measures that aim to raise the costs of malicious state behaviour. Second, the author highlights the importance of international cooperation related to devising concerted deterrence strategies and responses, continuously promoting norms of responsible state behaviour and sharing intelligence on the cyber threats.

The second chapter, written by the Estonian cybersecurity policy experts Kadri Kaska, Dr Liis Rebane and Toomas Vaks, focuses on the role of national cybersecurity strategies. Drawing from successes and failures based on the experience of developing three iterations of the Estonian cybersecurity strategy, the authors highlight practices and universal principles that have proven to be important to achieving positive impact. First, a nation needs to understand the strengths and weaknesses of the chosen governance model. In the Estonian case, a decentralised approach has yielded both negative and positive effects that need to be understood and taken into account at different levels of national policymaking. Second, it is naturally important that strategies are guided by agreed fundamental principles and a long-term vision. Third, a strategy cannot be only a set of high-level agreements – actionable and realistic objectives, together with defined metrics, are needed to support prioritisation of actions and to be able to measure success. Fourth, it has proved to be valuable for strategy development to be carried out as an inclusive process that brings together relevant national stakeholder groups to foster cooperation and build a stronger cybersecurity community. And last but not least, Estonia's experience has shown that national cybersecurity strategy needs to be openly communicated and accessible to international partners as a basis for and as a tool to support international dialogue and collaboration.

The third chapter of the report, by Dr Anna-Maria Osula, Senior Researcher at the Centre of Digital Forensics and Cyber Security at Tallinn University of Technology (TalTech) and Senior Policy Officer at Guardtime, examines Estonian and Japanese efforts to promote and build international norms of responsible state behaviour in cyberspace. It conceptualises Estonia as a promoter of cyber norms by explaining the unique motivations that drive small states to actively support the development of a stable international order. Nevertheless, when looking at activities and in international fora, it is clear that Japanese and Estonian interests converge to a very large extent: the nations have

common views on the applicability of international law, the relevance of implementing already agreed norms, and the opposition to establishing entirely new legally binding instruments for cybersecurity. Building on these commonalities, the author does not consider that differences in geography, history or size hinder the great potential for collaboration between Estonia and Japan in both bilateral and multilateral settings. In addition, cooperation should not be limited only to the level of international norms and diplomacy; it would be also beneficial to explore new ways to collaborate on more operational matters, such as exchanging threat intelligence, experiences in incident response, training frameworks, or engaging in confidence- and capacity-building activities.

The fourth and final chapter, by Dr Koichiro Komiyama, Visiting Fellow at Keio University Global Research Institute, addresses the operational aspects of cybersecurity cooperation by analysing relevant developments and the ongoing challenges related to the Computer Security Incident Response Team (CSIRT) community. It highlights that, although CSIRTs have been recognised as an important element in global cybersecurity governance, there are growing challenges that hinder effective international cooperation between the incident responders. It is clear that the intended role of the international CSIRT community – as a venue for cooperative response to global threats and for sharing technical and scientific knowledge – has been changing due to cybersecurity being increasingly guided by national security interests and geopolitical and commercial realities as well as new types of cyber threat. The author calls for a redefinition of the purpose and overall mandates of CSIRTs and highlights several development scenarios – ranging from adopting a model of an independent "cyber version" of the International Red Cross to the continuation of CSIRTs becoming fully governmental agencies and possibly ending up cooperating in "bubbles" formed on the basis of shared values and geopolitical interests. Whatever the scenario, it is clear that cybersecurity cooperation among like-minded countries – such as Japan and Estonia – is a pivotal enabler of effective collaboration between their CSIRTs.

List of Abbreviations

5G	Fifth Generation
AAE	Asia-Africa-Europe
AI	Artificial Intelligence
APEC	Asia-Pacific Economic Cooperation
APT	Advanced Persistent Threat
ASEAN	Association of Southeast Asian Nations
ATM	Automated Teller Machine
BRI	Belt and Road Initiative
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
C&C	Command and Control
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CDC	Center for Disease Control and Prevention
CERT/CC	Computer Emergency Response Team Coordination Centre
CPU	Central Processing Unit
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
DSR	Digital Silk Road
eID	Electronic Identity
EU	European Union
FBI	Federal Bureau of Investigation
FIRST	Forum of Incident Response and Security Teams
GCI	Global Cybersecurity Index
GGE	Group of Governmental Experts
IoT	Internet of Things
IT	Information Technology
ITU	International Telecommunications Union
JPS	Japan Pension Service
NATO	North Atlantic Treaty Organisation
ODA	Official Development Assistance
OEWG	Open-ended Working Group
OS	Operating System
OSCE	Organisation for Security and Cooperation in Europe
R&D	Research and Development
ROCA	Return of the Coppersmith Attack
SAIL	South Atlantic Inter Link
UN	United Nations
UNSC	United Nations Security Council
WHO	World Health Organisation

Editors' Introduction

Cooperation between Estonia and Japan has been growing steadily since the restoration of Estonia's independence in 1991 and encompasses economic, political, technological, cultural and security aspects. Since Estonia's accession to NATO and the EU in 2004, bilateral cooperation has also been supplemented with cooperation through the NATO-Japan and EU-Japan formats. Japan is a highly valued partner for these organisations, and Tallinn's efforts to advance its cooperation with Tokyo in bilateral and multilateral formats contributes to strengthening overall relations between NATO/EU and Japan.

Despite their significant differences rooted in history, culture and physical properties such as size and geographical location, the two countries share many security concerns. These particularly pertain to rising and revisionist powers in their immediate neighbourhood, erosion of multilateralism in international relations, rising geopolitical tensions that lead to military incidents and conflicts, potential destabilisation of cyberspace, and vulnerability of digital infrastructure. Estonia and Japan have also developed broadly similar approaches to addressing these sources of insecurity, such as: building credible self-defence capabilities; embedding themselves in multinational global and regional alliances; developing strong relations with the United States; protecting and further advancing international order based on rules and norms; and building the resilience of their critical national infrastructure.

Cybersecurity has emerged as an important area where Japan's and Estonia's concerns, interests and approaches are similar or even identical. Both nations are active in developing international norms for stability in cyberspace, ensuring multi-stakeholder governance of the internet and continuously updating their cybersecurity policies, practices and technologies to reflect trends in the threat environment. Both nations see Russia and China as actors behind many negative trends driving instability in cyberspace and thus threatening the national security of Estonia, Japan and other countries. And both nations see enhanced global, regional and bilateral cooperation between democracies as pivotal in shaping the cybersecurity landscape in ways that preserve their common values, prosperity and way of life.

Cybersecurity has emerged as an important area where Japan's and Estonia's concerns, interests and approaches are similar or even identical

With the aim of facilitating international cooperation through the exchange of national best practices and experience, this research report is devoted to sharing perspectives on Japan's and Estonia's cybersecurity policy. It is based on the proceedings of a webinar organised by the ICDS in February 2021, and explores, at greater length and in greater detail, several of the themes addressed during that event.

Chapter I provides an overview of the cyber threat landscape from a Japanese perspective, highlighting the different types of cyber operations that are actively undertaken by nation-states and the need to build comprehensive cyber deterrence that utilises principles of Active Cyber Defence. Chapter II focuses on the role of national cybersecurity strategies and, drawing from successes and failures based on the experience of developing three iterations of the Estonian cybersecurity strategy, highlights practices and universal principles that have proven to be important to the achievement of positive impact. Chapter III examines Estonian and Japanese efforts to promote and build international norms of responsible state behaviour in cyberspace, while Chapter IV addresses the operational aspects of cybersecurity cooperation by analysing relevant developments and the ongoing challenges related to the Computer Security Incident Response Team (CSIRT) community.

CHAPTER I

The Cyber Threat Landscape and Japan's Policy Challenges

JUN OSAWA

Introduction

In late January 2020, Mitsubishi Electric and NEC announced that data had been leaked from their systems as a result of a cyber-attack.[1] These two major Japanese electronics companies were likely attacked by the advanced persistent threat (APT) group known as "Tick" (also known as "Bronze Butler"), which has been targeting Taiwan and Japan since 2006. In addition to these two companies, Kobe Steel and Pasco, both of which have defence contracts with the Ministry of Defence, became victims of cyber-attacks.[2] According to analysis by Trend Micro, the group has targeted Japanese companies possessing advanced technologies in the domains of defence, aeronautics, chemicals and space (satellites).[3] It increased its activities in 2019 using new cyber-attack methods, breaking into internal networks through branch offices and subsidiary firms in China.

Over the last 15 years, it is apparent that states have been using cyberspace to achieve strategic goals and secure national interests. This trend began publicly in 2007 with cyber-attacks against Estonia.[4] In cyberspace, an intense state-to-state conflict in a realist world has emerged. Trends over the last decade reveal that cyber-attacks frequently correspond to incidents of international discord or conflict.

Trends over the last decade reveal that cyber-attacks frequently correspond to incidents of international discord or conflict

In the 2007 case in Estonia, a confrontation between Russia and Estonia over the removal of the Soviet-era statue known as "Bronze Soldier" triggered large-scale distributed denial-of-service (DDoS) attacks targeting the country's infrastructure.[5] State-sponsored cyber-attacks have also become a real threat not only to national security but also to the economic activities of the private sector. Cyber-attacks on critical infrastructure can paralyse state activity and cause the same human and material damage as a physical armed attack.

The purpose of this chapter is firstly to describe a Japanese perspective on the cyber

[1] NEC Corporation, "当社の社内サーバへの不正アクセスについて" [Unauthorised access to our internal server], press release, 31 January 2020, https://jpn.nec.com/press/202001/20200131_01.html; Mitsubishi Electric Corporation, "不正アクセスによる個人情報と企業機密の流出可能性について" [About the possibility of leakage of personal information and trade secrets due to unauthorised access], press release, 20 January 2020, https://www.mitsubishielectric.co.jp/news/2020/0120-b.pdf.

[2] Ministry of Defence of Japan, "防衛関連企業に対する不正アクセス事案について" [Unauthorised access to defence companies], press release, 6 February 2020, https://www.mod.go.jp/j/press/news/2020/02/06c.pdf.

[3] Joey Chen, Hiroyuki Kakara, and Masaoki Shoji, *Operation ENDTRADE: TICK's Multi-Stage Backdoors for Attacking Industries and Stealing Classified Data* (TrendMicro Research, 2019), https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf.

[4] Adam Segal defines the Estonian case as the first "cyber conflict". See: Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, NY: Public Affairs, 2016), 60.

[5] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York, NY: Harper Collins Publishers, 2010), 13–16.

Cyber espionage	Stealing confidential information, business secrets or intellectual property by employing sophisticated methods against specific targets
Cyber sabotage	Paralysing servers or network service temporarily, usually by an overwhelming volume of data traffic, using methods such as distributed denial of service (DDoS) attacks
Cyber subversion	Disrupting or destroying the operation of computer networks, including critical infrastructure, by means of deleting or manipulating digital data following intrusion of a network by employing sophisticated methods against specific targets
Cyber propaganda / manipulation	Distorting people's perceptions in order to manipulate public opinion, by means of supporting an information or influence operation, such as spreading fake news by proxy actors and disclosing cyber-stolen sensitive inside information
Ransomware and cyber theft	Targeted attacks to penetrate networks of certain government agencies, banks, companies and individuals to make unauthorised money transfers or to encrypt data to demand a ransom for its decryption
Military cyber-attacks	Disrupting or destroying an adversary's military cyber-based C4ISR assets or critical infrastructure along with military operations

Table 1. Main types of cyber-attack

threat landscape, in particular looking into which countries are trying to use cyber-attacks to realise their national interests, what kind of measures are employed, and what is the purpose of state-sponsored cyber-attacks against Japan. Secondly, the chapter discusses how to tackle state-sponsored cyber-attacks, and how nation-states try to shape strategies and policies that are helpful in stopping or deterring malevolent behaviour by states in the cyber domain. Thirdly, the chapter will outline options for future Estonian-Japanese cooperation in the cyber domain.

The number of cyber-attacks that appear to be state-sponsored has increased rapidly over the past decade, and the damage they cause has become increasingly severe

1. Types of Cyber-attacks Threatening National Security

In cyberspace, the number of cyber-attacks that appear to be state-sponsored has increased rapidly over the past decade, and the damage they cause has become increasingly severe. Some of these attacks have been impossible to prevent using only civilian cybersecurity measures. Until 2015, state-sponsored cyber-attacks could be mainly categorised as "cyber espionage", "cyber sabotage" or "cyber subversion", as shown in Table 1. As early as 2005, Japanese cybersecurity engineers identified "cyber espionage" operations that are targeted attacks aimed at stealing sensitive information and intellectual property from companies, government organisations and individuals (e.g. operations targeting policymakers or the defence industry). In addition to "cyber espionage", outside Japan, many countries faced state-sponsored cyber-attacks that fall into the category of "cyber sabotage" or "cyber subversion" operations.

However, since around 2015, new types of cyber-attack have emerged, such as "theft" or "ransom" attacks that infiltrate an organisation's network, aiming to make fraudulent money transfers or to demand a ransom for stolen and encrypted company data.

In addition, liberal democratic countries now face "propaganda/manipulation" cyber-attacks, which aim to manipulate the information space within a country by spreading fake news distributed by proxy entities, and to reveal stolen confidential

information, with the overall aim to distort people's perceptions and make people believe false "facts". This cyber-manipulation, for example to distribute or support "fake news", can have a significant impact on our democratic process. This type of attack could, in the worst case, sway the outcome of an election. For example, during the 2016 presidential election in the US, it is believed that Russian groups APT28 (FancyBear) and APT29 (CozyBear) conducted information-theft cyber-attacks and distributed internal information taken from the Democratic Party through Wikileaks.[6] Similar cyber-attacks took place in 2017 during the French presidential election and the German general election.[7] On an international level, Russia appears to be the most active in this kind of information warfare. In the East Asian region, China is also believed to be conducting such operations, but in Japan there are currently no obvious signs of information warfare by either Russia or China, possibly due to the Japanese language barrier.

Four countries – Russia, China, North Korea and Iran – are actively engaged in cyber-attacks that deviate from existing international rules and norms and pose significant security threats

It is clear that almost all major countries are involved in offensive activities in cyberspace, as exemplified by the creation of "cyber armies" or dedicated units to conduct cyber operations. Four of these countries – Russia, China, North Korea and Iran – are actively engaged in cyber-attacks that deviate from existing international rules and norms and pose significant security threats. In its National Cyber Strategy, published in September 2018, the US clearly identified these four countries as adversaries who "use cyber tools to undermine our economy and democracy, steal our intellectual property, and sow discord in our democratic processes".[8] Table 2 summarises the main types of cyber-attack in which these countries are alleged to have been involved.

Cyber espionage	China, Russia
Cyber sabotage	Russia, North Korea
Cyber subversion	Russia, North Korea, Iran
Ransomware and cyber theft	North Korea
Cyber propaganda/ manipulation	Russia, China

Table 2. Types of cyber-attack and main suspected perpetrators

Although it is evident that democratic countries also engage in different types of offensive cyber operations (e.g. cyber espionage or subversion, such as Stuxnet against Iranian nuclear facilities), from the viewpoint of threats to democratic countries' national security, cyber activities by the aforementioned four countries are the most relevant to consider.[9]

Cyber-attacks conducted by Russia are generally characterised as (1) cyber sabotage or subversion attacks against neighbouring countries, (2) "hybrid warfare" in its military operations, (3) cyber espionage, especially against US and European countries, and (4) cyber propaganda/manipulation, or information warfare, against democratic countries.

Cyber-attacks conducted by China predominantly fall into the category of cyber espionage. China actively uses cyberspace to

[6] US Department of Homeland Security and Federal Bureau of Investigations, "Grizzly Steppe – Russian Malicious Cyber Activity," 29 December 2016, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf; also see: Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," 6 January 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[7] US Department of Justice Office of Public Affairs, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," press release, 19 October 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and; Jeffrey Mankoff, "Russian Influence Operations in Germany and Their Effect," CSIS Commentary, Center for Strategic and International Studies (CSIS), 3 February 2020, https://www.csis.org/analysis/russian-influence-operations-germany-and-their-effect.

[8] The White House, *National Cyber Strategy of the United States of America* (Washington, DC: The White House, 2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[9] David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York, NY: Crown Publisher, 2012); Kim Zetter, *Countdown to ZeroDay: Stuxnet and the Launch of the World's First Digital Weapon* (New York, NY: Crown Publishers, 2014).

steal (1) policy information held by government agencies of other countries, (2) intellectual property that contributes to the development of Chinese science and technology, and (3) trade secrets that give Chinese companies a business advantage. In addition, it is reported that China has been conducting "cyber propaganda/manipulation" attacks similar to those of Russia, mainly in the Asian region.[10]

Until around 2015, North Korea engaged in disruptive "sabotage" or "subversion" cyber-attacks against South Korea and the US, but more recently Pyongyang has been conducting "ransom" cyber-attacks to make up for the shortage of foreign currency caused by UN economic sanctions.[11] Iranian cyber-attacks have been characterised as "subversion", directed mainly at the US and Sunni Gulf states.[12]

Activities by China and North Korea have been the most alarming threats for Japan, but in 2020 Russia has also become a concern. In the autumn of that year, for example, it was revealed that Russia was targeting the Tokyo 2020 Olympics with a "denial of function" or "disruption" type of attack.[13] The next section details the cyber threats from a Japanese perspective.

Activities by China and North Korea have been the most alarming threats for Japan, but in 2020 Russia has also become a concern

2. Japanese Cyber Threat Landscape

2.1. Cyber espionage and "Made in China 2025"

China is one of the leading countries using cyberspace for strategic goals. Chinese cyber espionage targets almost all other countries to steal secret government information, business secrets and intellectual property.[14]

In Japan, a large-scale targeted attack by an APT aimed at stealing information from the House of Representatives, government institutions and the defence industry came to light in 2011.[15] Similar attacks with the objective of stealing information are believed to have taken place since around 2005.[16] In May 2015, a targeted cyber-attack using Emdivi malware took place against the Japan Pension Service (JPS), with the first wave hitting on 8 May 2015. Four more waves followed over the next two weeks, infecting more than 30 computers and leaking personal information on 1.25 million individuals within one day, caused by a cyber operation conducted from somewhere outside the country.[17] A technical analysis of the malware concluded that its creator was a group of people in China who worked between 9 a.m. to 5 p.m. from Monday to Friday.[18] Thus, there is a strong suspicion that a government entity was involved.

[10] Tomoko Nagasako, "Global disinformation campaigns and legal challenges," *International Cybersecurity Law Review,* 1 (2020): 125-36.

[11] Jenny Jun, Scott LaFoy and Ethan Sohn, *North Korea's Cyber Operation: Strategy and Response* (CSIS Korea Chair Report) (Washington, DC: Center for Strategic and International Studies, 2015), http://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf; United Nations Security Council Panel of Experts, *Midterm report of the Panel of Experts Submitted Pursuant to Resolution 2464 (2019)* (New York, NY: United Nations, 2019), https://undocs.org/S/2020/151.

[12] Iran Action Group and Iran Office of the Bureau for Near Eastern Affairs, *Outlaw Regime: A Chronicle of Iran's Destructive Activities* (2020 Edition) (Washington, DC: US Department of State, 2020), https://www.state.gov/wp-content/uploads/2020/09/Outlaw-Regime-2020-A-Chronicle-of-Irans-Destabilizing-Activity.pdf.

[13] UK Foreign, Commonwealth and Development Office, "UK exposes series of Russian cyber attacks against Olympic and Paralympic Games," press release, GOV.uk, 19 October 2020, https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games.

[14] Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (Oxford: Oxford University Press, 2015); Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Santa Barbara, CA: Praeger, 2016).

[15] "Japan defence firm Mitsubishi Heavy in cyber attack," *BBC News*, 20 September 2011, https://www.bbc.com/news/world-asia-pacific-14982906; Martin Fackler, "Virus Infects Computers in Japan's Parliament," *The New York Times*, 25 October 2011, https://www.nytimes.com/2011/10/26/world/asia/virus-infects-computers-in-japans-parliament.html.

[16] IPA, *標的型攻撃メールの分析に関するレポート* [Report on the analysis of targeted attack emails] (IPA, 2011), 6, https://www.ipa.go.jp/files/000009375.pdf.

[17] National Center of Incident Readiness and Strategy for Cybersecurity (NISC), "日本年金機構における個人情報流出事案に関する 原因究明調査結果" [Results of the investigation into the cause of the leak of personal information at the Japan Pension Service], 20 August 2015, https://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf.

[18] Macnica Networks, *標的型攻撃の実態と対策アプローチ* [The reality of targeted attacks: Counter-measures approach] (Macnica Networks Corporation, 2016), https://www.macnica.net/file/security_report_20160613.pdf.

Name of APT group	Targets (country and industries)
APT1	English-speaking countries: government, **IT**, financial, **energy**, etc.
APT4	Asia-Pacific countries (Japan and South Korea): **aerospace** and defence industry
APT5	South-East Asian countries, now worldwide: **telecoms**, **IT**, **high-tech**, defence industry
APT9 (Nightshade Panda)	US, Japan, Taiwan, Singapore, India, South Korea and Thailand: **aerospace**, **agriculture**, construction, **energy**, **medical**, **transportation**
APT10 (Cloud Hopper)	Worldwide (since 2016, esp. Japan): government, think-tanks, media, **aerospace**, defence industry, **medical and healthcare**
Cloudy Omega/Blue Termite	Japan: government, academia, financial, **energy**, chemicals, heavy industry, media, **IT**, etc.
APT12 (Numbered Panda)	Asia-Pacific countries (to 2011), Taiwan and Japan (since 2011): defence industry (**satellite, encryption** and **aerospace**)
APT15	Europe and US: trade, financial, **energy**, defence industry
APT16	Taiwan and Japan: government, media, financial, **high-tech**
APT17 (Hidden Lynx)	Worldwide (since 2016, esp. Japan): government, **IT**, **aviation**, law firms
Dragon OK	Japan: academia (science and technology)
Tick (Bronze Butler)	Japan: **high-tech**, chemicals, heavy industry (shipbuilding), media
APT41/Winnti	US, Australia, South Korea, UK and Japan: **high-tech**, chemicals, **e-commerce**, financial, **electronics**, **telecoms**, **healthcare**, **pharmaceutical**, gaming industry
Black Tech (PLEAD)	Taiwan and Japan: **high-tech**, financial, government
Taiddor	Taiwan, Japan (since 2017) and US (since 2019): government, academia, defence industry
Tonto	Taiwan, Russia and Japan: defence industry, automotive, media, think-tanks

Compiled by the author from various published sources and discussion with cybersecurity engineers in Japan. For explanation of use of bold, see main text.

Table 3. Chinese APT groups and cyber espionage operations

According to analysis by FireEye, Chinese state-sponsored "cyber espionage" attacks have been particularly aggressive against Japan since 2016, with at least 10 more Chinese-linked APT groups, as shown in Table 3, targeting the country.[19] Intellectual property and trade secrets in advanced industries such as defence, aerospace, high-tech and pharmaceuticals have been targeted.

From Table 3, we can conclude that the victims targeted by the listed Chinese cyber-espionage groups are industries and business entities developing cutting-edge technologies that appear on the list in China's recent manufacturing strategy "Made in China 2025" as ten key sectors (industries listed in the strategy are indicated in bold).[20] It can thus be claimed that these cyber-espionage activities are linked

[19] FireEye, "APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat," FireEye Blog, 6 April 2017, https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html.

[20] US Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections* (Washington, DC: US Chamber of Commerce, 2017), https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf.

to China's long-term strategy for seeking technological and economic supremacy. There is a risk of long-term and strategic "technology leakage", which would ultimately damage Japan's industrial competitiveness. Thus, it is clear that the cyber domain has become a real battleground over economic security between China and developed Western countries, including Japan.

The cyber domain has become a real battleground over economic security between China and developed Western countries, including Japan

2.2. DPRK: ANOTHER CYBER THREAT ACTOR IN EAST ASIA

North Korea is another significant actor engaged in cyber-attacks in East Asia. For example, South Korea faced severe and sophisticated cyber-attacks in 2013. On the afternoon of 20 March, the internal computer networks of television broadcasters and three major banks were forced to shut down, caused by a premeditated malware assault on servers and tens of thousands of computers in the networks.[21] The banks' ATMs and the broadcasters' news distribution systems were paralysed for several hours. South Korea's official investigation blamed North Korea for being behind the cyber-attacks.[22]

A year later, in November 2014, Sony Pictures Entertainment was targeted by a hacking group self-proclaimed as the "Guardians of Peace".[23] The FBI started an investigation soon after the attack and confirmed a month later that North Korea was behind it.[24] The Obama administration officially blamed North Korea; the then Secretary of Homeland Security, Jeh Johnson, stated that the attack was an attack not just against a company and employees, but also on the United States' freedom of speech and way of life, and as a result tightened sanctions against North Korea.[25] In addition, the distributed malware "Wannacry" that spread in computer networks around the world in May 2017 – infecting more than 300,000 computers in 150 countries within 10 days – was linked to North Korea.[26]

In recent years, North Korean groups have been targeting the financial sector to gain funds to preserve the country's internationally isolated regime. For instance, the UN Security Council Panel of Experts estimates that North Korea had obtained $2 billion through cyber-attacks on the financial sector, including from cryptocurrency.[27] A series of attacks targeting cryptocurrency exchanges was uncovered in Japan, and thus the North Korean "money-oriented" cyber-attack is of increasing concern.[28]

In recent years, North Korean groups have been targeting the financial sector to gain funds to preserve the country's internationally isolated regime

[21] Zachary Keck, "South Korea Hit by Cyber Attack – North Korea to Blame?," *The Diplomat*, 21 March 2013, https://thediplomat.com/2013/03/south-korea-hit-by-cyber-attack-north-korea-to-blame/.

[22] Lee Minji, "Gov't confirms Pyongyang link in March cyber attacks," *Yonhap News*, 10 April 2013, https://en.yna.co.kr/view/AEN20130410007352320.

[23] TrendMicro, "The Hack of Sony Pictures: What We Know and What You Need to Know," 8 December 2014, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know.

[24] Federal Bureau of Investigations (FBI), "Update on Sony Investigation," press release, 19 December 2014, https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

[25] David E. Sanger, Michael S. Schmidt, and Nicole Perlroth, "Obama Vows a Response to Cyberattack on Sony," *The New York Times,* 19 December 2014, https://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html.

[26] U.S. Department of Justice Office of Public Affairs, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," 17 February 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

[27] United Nations Security Council Panel of Experts, *Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)* (New York, NY: United Nations, 2010), https://www.undocs.org/S/2010/571.

[28] Reuters, "North Korean hackers said possibly behind massive Coincheck heist," *The Japan Times*, 6 February 2018, https://www.japantimes.co.jp/news/2018/02/06/business/tech/north-korean-hackers-said-possibly-behind-massive-coincheck-heist/.

3. The Contest for Supremacy in Digital Infrastructure

Adding to the struggle in the cyber domain, there is a global battle over digital infrastructure construction that is of strategic relevance to Japan. With the arrival of the age of the IoT (Internet of Things), known as the fourth industrial revolution, a fierce battle for digital supremacy is breaking out between the US and China over communications infrastructure such as fifth-generation (5G) mobile communications networks and various other IoT platforms and enablers.

A fierce battle for digital supremacy is breaking out between the US and China

China is attempting to break US digital dominance by launching a digital version of its Belt and Road Initiative (BRI), the "Digital Silk Road" (DSR). In 2015, Beijing introduced the DSR as part of the renowned BRI, to improve the communications connectivity of Eurasian countries and China. In 2017, Beijing expanded the concept of the DSR to the field of IoT platforms, for example related to e-commerce, digital payments, social networking services and digital surveillance systems.[29]

On the "hardware" side, China telecoms launched the Transit Silk Road cable between China and Europe in 2016.[30] On the maritime front, China Unicom has laid submarine cables, including the AAE-1 cable between China and Europe and the SAIL cable across the South Atlantic between Brazil and Cameroon, which was in service by 2018.[31] Furthermore, Huawei's subsidiary, Huawei Marine, is laying a submarine cable around Africa, and planned to open a "Peace Cable" between East African countries in 2019.[32]

On the "software" side, smartphone-based electronic payment platforms are already spreading across South-East Asia and India. Ant Financial, an Alibaba Group company, has exported its systems to India, Thailand, South Korea, the Philippines, Malaysia, Indonesia, Pakistan and Bangladesh.[33] A memorandum of understanding to strengthen cooperation in the construction of the DSR, which includes the adoption of Chinese standards in e-commerce and e-payments, has been signed with 16 countries along the route of the BRI.[34] Chinese digital surveillance systems based on Chinese artificial intelligence (AI) technology have been exported to 63 countries around the world, 36 of which are BRI partner countries.[35]

In this way, China's "Digital Silk Road" concept is based both on the "hardware" (physical layer) of information and communications infrastructure and the "software" (logical layer) of the IoT platforms, which is designed to enclose the world's information data flow within a digital network made in China, build

China's "Digital Silk Road" is designed to enclose the world's information data flow within a digital network made in China, build a dominant position in cyberspace in the fourth industrial revolution, and seize digital hegemony from the US

[29] Ministry of Foreign Affairs of the People's Republic of China, "Full text of President Xi's speech at opening of Belt and Road forum," 15 May 2017, https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1465819.shtml.

[30] China Telecom, "Euro-Asia Network Solution," n.d., https://www.chinatelecomeurope.com/wp-content/uploads/ChinaTelecom_Euro-Asia-network-solution.pdf.

[31] Gary Maidment, "SAIL the Atlantic with CAMTEL," *WinWin*, 21 April 2018, https://www.huawei.com/en/publications/winwin-magazine/31/sail-the-atlantic-with-camtel.

[32] Huawei, "Huawei Marine and Tropical Science Commences Work on the Construction of the PEACE Submarine Cable Linking South Asia with East Africa," 6 November 2017, https://www.huawei.com/en/news/2017/11/PEACE-Submarine-Cable-SouthAsia-EastAfrica.

[33] Daniel Keyes and Greg Magana, "REPORT: Chinese fintechs like Ant Financial's Alipay and Tencent's WeChat are rapidly growing their financial services ecosystems," *Business Insider*, 19 December 2019, https://www.businessinsider.com/china-fintech-alipay-wechat.

[34] One Belt, One Road Construction Business Promotion Guidance Group Benkou Office, 「一帯一路」共同建設のイニシアチブ 進展、貢献と展望 *2019* [The "One Belt, One Road" Joint Construction Initiative: Progress, Contributions and Prospects 2019] (Beijing: China International Book Trading Co, 2019), https://www.yidaiyilu.gov.cn/wcm.files/upload/CMSydylgw/201904/201904240813002.pdf.

[35] Steven Feldstein, "The Global Expansion of AI Surveillance," Working Paper, Carnegie Endowment for International Peace, September 2019, https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.

a dominant position in cyberspace in the fourth industrial revolution, and seize digital hegemony from the US.

Although Chinese president Xi Jinping defended the BRI by stating that "China has no geopolitical calculations" in his keynote speech at the Boao Forum in April 2018, the initiative is regarded as a geopolitical strategy by Western scholars and strategists.[36] The BRI/DSR encompasses entire coastal areas of the Eurasian continent from East Asia to Western Europe – an area referred to as "Rimland" by the US strategist Nicholas Spykman: "Who controls the Rimland rules Eurasia, who rules Eurasia controls the destinies of the world". [37]

Thus, IT infrastructure building and IoT platforms, including the "rivalry" between the 5G Clean Path (the US initiative) and the DSR, have become another field of international competition for global digital dominance between the US and China. As a military ally of the US, similar to NATO countries, Japan has to set out a plan for 5G networks and digital platforms to address supply chain risks created by the DSR.

4. How to Deter State-Sponsored Cyber Attacks?

It is not enough for the private sector alone to respond to these new dimensions of cyber-attacks, which are state-sponsored and utilise state-of-the-art techniques. It is essential for states to take the lead in fulfilling their responsibilities in order to deter potential state adversaries conducting cyber-attacks that go against national interests. Until now, the national response to cyber-attacks has focused on "passive cyber-defence" such as protecting government networks and infrastructure with measures such as patches, end-point security, firewalls and intrusion detection systems to mitigate cyber-attacks and reduce systems' vulnerability. These measures of passive defence are now clearly insufficient.

To prevent potential state adversaries from conducting cyber-attacks against national interests, democratic allies must employ a new strategy based on "comprehensive cyber deterrence".[38] The cyber domain is a world in which the attacker has the overwhelming advantage. Defensive measures alone are therefore not enough to prevent sophisticated cyber-attacks. It is important for defences to increase the cost of carrying out an attack and to create an environment in which attackers are hesitant. To do so, it is necessary to enhance both "cyber deterrence by denial" capability by increasing the level of cybersecurity to ensure resistance and resilience, and "cyber deterrence by punishment" capability by various means including cyber counterattacks, to deter advanced state-sponsored cyber-attacks. Ensuring cybersecurity through such deterrence measures is not limited to activities in cyberspace. It requires the mobilisation of all policy tools, including naming and shaming, coordinated diplomatic pressure, sanctions and judicial prosecutions against aggressors.[39] As an example, the US has employed a new

Measures of passive defence are now clearly insufficient. To prevent potential state adversaries from conducting cyber-attacks against national interests, democratic allies must employ a new strategy based on "comprehensive cyber deterrence"

[36] "Transcript: President Xi Addresses the 2018 Boao Forum for Asia in Hainan," US-China Perception Monitor, 18 April 2018, https://uscnpm.org/2018/04/11/transcript-president-xi-addresses-2018-boao-forum-asia-hainan/.

[37] Nicolas J. Spykman, *The Geography of the Peace* (New York, NY: Harcourt, Brace & Co., 1944), 43.

[38] Regarding the concept of cyber deterrence, see: Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3 (Winter 2016/17): 44–71; Jun Osawa, "The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?," *Asia-Pacific Review,* vol. 24, No. 2 (2017): 113-31. Scott Jasper, *Strategic Cyber Deterrence* (Lanham, MD: Rowman & Littlefield, 2017).

[39] Adam Botek, "European Union establishes a sanction regime for cyber-attacks," *INCYDER*, NATO Cooperative Cyber Defence Centre of Excellence, 10 October 2019, https://ccdcoe.org/incyder-articles/european-union-establishes-a-sanction-regime-for-cyber-attacks/; Chris Painter, "Deterrence in cyberspace. Spare the costs, spoil the bad state actor: Deterrence in cyber space requires consequences," ASPI Policy Brief / Report No. 4, The Australian Strategic Policy Institute, 2018, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2018-05/Deterrence%20in%20cyberspace_0.pdf?JtY9WhXLd53pCnni2U5PiHr8ikcPMC5I.

strategy of "cyber deterrence" in which it applies deterrence theory to the cyber domain. The US Department of Defense's Cyber Strategy for 2015 called for "deterrence in the Future Security Environment", stating that "the Department of Defense must contribute to the development and implementation of a comprehensive cyber deterrence strategy to deter key state and non-state cyber actors from conducting cyber-attacks against U.S. interests".[40] Since then, Washington has adopted various policy tools that could deter state-sponsored cyber-attacks. For instance, as a response to cyber-espionage operations from China, the US Department of Justice prosecuted five Chinese military officers in 2014.[41]

Tokyo has also adopted this new strategy of cyber deterrence. In its 2018 Cybersecurity Strategy, the Government of Japan decided to promote the policy of "Active Cyber Defence" – a concept that "describes a range of proactive actions that engage the adversary before and during a cyber incident", or that "ensures the government to [sic] implement active preventive measures against threats in advance".[42] The 2018 Strategy also introduced the idea of comprehensive cyber deterrence and active cyber defence, as follows: "in order to deter malicious cyber activities …, Japan will utilize political, economic, technological, legal, diplomatic, and all other viable and effective means and capabilities, depending on the threat, and take resolute responses against cyber threats that undermine our national security, including those possibly state-sponsored".[43]

In the policy, the Japanese government emphasises three pillars of necessary capabilities to "defend the state (defence capabilities), deter cyberattacks (deterrence capabilities), and be aware of the situation in cyberspace (situational awareness capabilities)".[44]

A more active cyber defence by means such as continuous monitoring of APT groups and responses to attacks is now required

A more active cyber defence by means such as continuous monitoring of APT groups and responses to attacks is now required. To do that, monitoring activities of cyber adversaries, accumulating vast amounts of electronic information from the Internet, conducting post-event analysis and follow-up using big data analysis are needed.

Active Cyber Defence is required to monitor and respond to cyber-attacks as soon as possible. New cyber threats require a national response, as it is difficult for private companies and private cybersecurity industries to cope with aspects such as continuous monitoring of attack groups' activities and the response to attacks. Acknowledging that it is a legally controversial topic to introduce counter-attack measures (such as hack-backs), it is nevertheless necessary in some cases to intrude into the cyber assets of adversaries, such as C&C servers, to monitor and analyse their behaviour before and during cyber incidents.[45] These active cyber defence measures, such as monitoring data flow and identifying the attackers, should be carried

[40] US Department of Defense, *The DoD Cyber Strategy* (Washington, DC: Department of Defense, 2015), 10, https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.

[41] US Department of Justice Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," news release, 19 May 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[42] Government of Japan, *Cybersecurity Strategy 2018* (Tokyo: NISC, 2018), https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf. Regarding to the concept of "active cyber defence", see: William A. Owens, Kenneth W. Dam, and Herbert S. Lin (eds.), *Technology, Policy, Law, and Ethics. Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: The National Academies Press, 2009), https://doi.org/10.17226/12651; Robert M. Lee, "The Sliding Scale of Cyber Security," SANS Analyst White Paper, SANS Institute, August 2015, https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240; Center for Cyber and Homeland Security, *Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats* (Washington, DC: The George Washington University, 2016), https://wayback.archive-it.org/5184/20190103002934/https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf; Irving Lachow, "Active Cyber Defense: A Framework for Policymakers," CNAS Policy Brief, Center for a New American Security, February 2013, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS_ActiveCyberDefense_Lachow_0.pdf?mtime=20160906080446&focal=none.

[43] Government of Japan, *Cybersecurity Strategy 2018*, 39.

[44] Ibid, 37.

[45] Nicholas Winstead, "Hack-Back: Toward a Legal Framework for Cyber Self-Defense," Center for Security, Innovation, and New Technology, American University, 26 June 2020, https://www.american.edu/sis/centers/security-technology/hack-back-toward-a-legal-framework-for-cyber-self-defense.cfm.

out by national government agencies as part of their legitimate activities, under adequate supervision by civil society.

Conclusions

State-sponsored cyber-attacks have become a serious threat to national security. In Japan, as in other technologically advanced countries, attacks targeting intellectual property and business secrets are damaging industrial competitiveness and shaking the backbone of the nation's economic strength. One of the reasons "rogue" states that engage in offensive cyber operations are able to "roam freely" in cyberspace is the absence of an internationally agreed mechanism to constrain undesirable behaviour by states, such as cyber espionage against the private sector, disruptive cyber-attacks against critical infrastructure, and cyber manipulation against democratic processes. Such a mechanism would give the international community the necessary legitimacy to engage in substantial counter-attacks against actors who do not comply with internationally agreed norms and engage in prohibited activities.

One of the reasons "rogue" states that engage in offensive cyber operations are able to "roam freely" in cyberspace is the absence of an internationally agreed mechanism to constrain undesirable behaviour by states

In order to stop state-sponsored cyber-attacks, some countries, such as the US and the UK, have begun to adopt active cyber defence as a policy, imposing costs on cyber-attackers based on the idea of cyber deterrence. At a time when cyber-attacks are becoming increasingly damaging and threatening our democratic processes, we need to seriously consider undertaking active cyber defence based on the concept of comprehensive cyber deterrence.

Estonia and Japan are located in the Eurasian "Rimland", with large neighbouring countries that can be regarded as two of the world's most notorious states in terms of offensive activities in cyberspace. Is it possible for Estonia and Japan to deal with threats from such advanced cyber powers?

As liberal democracies sharing fundamental values such as freedom, democracy, a market economy, human rights and the rule of law, it is clear that the two countries have the potential to cooperate in safeguarding international security in cyberspace, through cooperation in the following three areas:

- To increase stability in cyberspace, Estonia and Japan could collaboratively **promote norms of state behaviour in cyberspace**, such as refraining from cyber-enabled theft of intellectual property for commercial gain, not attacking critical infrastructure and not interfering in internal affairs by means of cyber manipulation. If state-sponsored attackers do not comply with internationally agreed norms and commit acts on the list of prohibited activities, the international community will gain legitimacy to launch stronger countermeasures as part of a policy of active cyber defence.

- In order to protect cyberspace, early detection of cyber-attacks is essential, and warnings must be shared without delay among like-minded countries. Estonia and Japan could make effective use of **cyber threat intelligence sharing** by means of exchanging views on cyber threat situational awareness and the activities of potential cyber adversaries, through both intergovernmental meetings and opportunities such as the exchange of indications of compromise on cyber-attacks held by national Computer Emergency Response Teams (CERTs).

- To make good use of diplomatic measures, Estonia and Japan could consider taking a **concerted diplomatic posture against the malicious behaviour** of their neighbouring powers in cyberspace, e.g. an internationally coordinated condemnation of the Chinese state-sponsored APT 10 cyber operation in December 2018. In order to exercise such diplomatic pressure, both countries need to identify cyber-attacks that pose a common threat and coordinate between diplomatic authorities. It would be useful to discuss cyber situational awareness in the cyber cooperation talks between Estonia and Japan, focusing on common cyber threats.

CHAPTER II

Lessons from Estonia's National Cybersecurity Strategy: How to Succeed or Fail in Delivering Value

Kadri Kaska
Liis Rebane
Toomas Vaks

Introduction

Estonia has built its current level of cybersecurity maturity over the past 12 years by the continuous and systematic implementation of cybersecurity measures, supervision and collaboration; by relying on a decentralised governance model; guided by three national cybersecurity strategies, and verified through two national-level cyber crises in 2007 and 2017.

Estonia's digital ecosystem relies on the government-ensured secure digital identity and secure interagency data exchange environment. This approach has served as the enabler and amplifier of rapid digital innovation and ensured that cybersecurity is integrated into the very foundations of the digital society

Estonia's digital ecosystem relies on the government-ensured secure digital identity and secure interagency data exchange environment. This approach has served as the enabler and amplifier of rapid digital innovation and ensured that cybersecurity is integrated into the very foundations of the digital society. On the policy level, however, its decentralised cybersecurity governance model, in which stakeholders retain broad independence, has posed systemic challenges leading to weak coherence in strategic cybersecurity management and coordination, and ambiguous division of roles and responsibilities across organisations' overlapping mandates. Paradoxically, this lack of a centralised formal governance structure has simultaneously enabled an agile, flexible and integrated community, proven to serve as one of Estonia's greatest assets.

Lessons from Estonia's experience in building its cyber resilience alongside the development of the digital society, supported by national-level strategic planning, do not appear to be limited to Estonia. After giving an overview of Estonia's three national cybersecurity strategy periods, this chapter aims to draw some universally applicable lessons by discussing practical deliverables of cybersecurity strategies and the ways they offer to succeed or fail in creating real value.

1. Evolution of Estonia's National Cybersecurity Strategy

Estonia's first cybersecurity strategy, issued in May 2008, was driven by a manifest and well-recognised national need: lessons from the large-scale cyberattacks in the spring of 2007, when political tensions between Estonia and Russia spilled over into cyberspace and triggered weeks of coordinated cyber-attacks against Estonia's online presence – financial institutions, government agencies, news media and communications infrastructure.[1] The attacks brought about two important lessons for the Estonian state and society: (1) that targeting online assets can have a tangible impact on modern society's sense of normality, and (2) that, despite the onslaught, the country could maintain its functioning society and "the digital way of life" with the support of its existing fundamental technical, institutional and legal frameworks, and by connecting to international incident cooperation networks.[2] Following these lessons, the 2008 strategy was based on a firm recognition that national cybersecurity is a comprehensive task comprising public–private action, various domains, and technical, organisational and legal measures. The strategy focused on addressing resilience gaps by improving the cybersecurity of essential services, while institutionalising the experienced success of public–private collaboration and international cooperation.

The 2008 strategy was based on a firm recognition that national cybersecurity is a comprehensive task comprising public-private action, various domains, and technical, organisational and legal measures

The first strategy set the foundation for Estonia's overall cybersecurity model by: (1) improving infrastructure resilience, (2) allocating roles and responsibilities, (3) establishing the notion of a comprehensive national cybersecurity toolbox encompassing technology, legal framework, organisations and processes, and (4) placing a strong emphasis on international cooperation. Its successor, in 2014, set out to build further national detection and response capabilities; emphasised cybersecurity education and research as means for future-proofing society against cyber threats, addressed the national defence dimension of cybersecurity, and introduced a set of common principles to support a consistent cybersecurity approach across stakeholders and areas of responsibility.[3] The 2019 strategy, informed by the lessons of the 2017 ROCA (Return of the Coppersmith Attack) eID (electronic identity) vulnerability crisis, created mechanisms to stimulate the development of a strong, R&D-based cybersecurity enterprise sector, outlined objectives to fulfil Estonia's ambition in promoting the rule of law and norms of responsible state behaviour internationally,

Estonia's fourth national cybersecurity strategy is currently under development and is expected to merge the strategic planning of cybersecurity with the national digital agenda for the next decade

[1] Cyber Security Strategy Committee of Estonia, *Cyber Security Strategy* (Tallinn: Ministry of Defence, 2008), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy/@@download_version/993354831bfc4d689c20492459f8a086/file_en. For a more detailed account of and background to the events, see Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010), 18–23, https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf.

[2] Estonian Information System Authority, *Annual Cyber Security Assessment 2017* (Tallinn: Estonian Information System Authority, 2017), 4–5, https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria_csa_2017.pdf.

[3] Ministry of Economic Affairs and Communications of Estonia, *Cyber Security Strategy 2014-2017* (Tallinn: Ministry of Economic Affairs and Communications, 2014), https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.

and substantiated the country's ambition towards a skilled society and workforce.[4]

Estonia's fourth national cybersecurity strategy is currently under development and is expected to merge the strategic planning of cybersecurity with the national digital agenda for the next decade. This step aims to complete establishing cybersecurity planning as a fully integrated part of the development of the digital society.[5]

2. Delivering Practical Outcomes?

Deriving from Estonia's experience over the past dozen years, five practical national cybersecurity strategy deliverables can be identified that have, to varying degrees of success, reinforced Estonia's development as a resilient digital society:

- a coherent and efficient **governance model** that is realistic with regard to available resources;
- a **strategic vision** and a set of fundamental principles ensuring long-term, value-driven development of national cybersecurity;
- a set of strategic objectives **along with an action pl**an for the strategy period, ensuring coordinated prioritisation and sustained progress in tackling increasing technological challenges and cyber threats;
- executing **national cybersecurity strategy planning as a process** that incorporates relevant actors across the whole cyber ecosystem, thereby strengthening the cybersecurity community by improving its interoperability and mutual calibration;
- making the strategy **accessible to international partners** by disclosing the proposed activities and underlying process, thereby offering a tool to support dialogue and collaboration with international counterparts.

While these deliverables correlate to some degree, each can be studied – and achieved – independently, as none is a strong prerequisite for the others. Each of these has its challenges, as the Estonian experience amply exemplifies. The following subsections describe the deliverables, discussing their impact, challenges, lessons learnt, and overall insight acquired from Estonia's three cybersecurity strategy documents and their implementation periods.

The 2018 review of the state of Estonia's cybersecurity affairs highlighted two key shortcomings: a lack of coherent leadership and a lack of ownership

2.1. A functional governance model

The 2018 review of the state of Estonia's cybersecurity affairs highlighted two key shortcomings: a lack of coherent leadership – where national cybersecurity resembled the sum of individual agencies' activities according to their own priorities more than a concerted whole – and a lack of ownership, with cybersecurity viewed as a complex technical matter that someone else should deal with. Consequently there was insufficient cross-agency situational awareness and information exchange, as well as fragmented, uneven and often wasteful cybersecurity management, despite general policy guidelines suggesting the consolidation of resources.[6] The 2021 draft strategy appears to come to similar conclusions, citing the challenge of ensuring adequate resources (primarily personnel) to effectively run a decentralised system in an increasingly complex environment, and ambiguity of responsibilities beyond broadly drawn roles.[7]

[4] See Estonian Information System Authority, "ROCA Vulnerability and eID: Lessons Learned," n.d., https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf; Ministry of Economic Affairs and Communications of Estonia, *Cybersecurity Strategy 2019-2022: Republic of Estonia* (Tallinn: Ministry of Economic Affairs and Communications, 2019), https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

[5] The draft *Digital Society Development Plan 2030* was released for consultations with stakeholders in late autumn 2020. There is no publicly available version at the time of writing this chapter.

[6] Ministry of Economic Affairs and Communications of Estonia, *Cybersecurity Strategy 2019-2022,* Section 1.3.

[7] Draft *Digital Society Development Plan 2030.*

Clearly defined cybersecurity roles and accountability across the "whole of system" are generally recognised as fundamental for successful governance, and most national cybersecurity strategies devote a substantial amount of attention to this topic.[8] Actual national models vary; most adopt the approach of individual responsibility allocation with some cyber-specific coordination body aligning their (cyber) activities.[9] Estonia's reliance on a decentralised model, with stakeholders retaining their independence and the role of the lead body (the Ministry of Economic Affairs and Communications) as primus inter pares generally weak, has meant that achieving consistency of priorities, approach and resources across sectors has remained a persistent struggle. The National Cybersecurity Council, consisting of representatives of relevant ministries, is a policy planning and coordination format reflecting the same "sum of individual parts" approach, with individual ministries enjoying broad autonomy in their planning and working programmes.

The divergent interests of different agencies and ministries (the notorious "silo" approach) and difficulties in achieving central coordination have proven the main roadblocks to meeting strategic objectives

The divergent interests of different agencies and ministries (the notorious "silo" approach) and difficulties in achieving central coordination have proven the main roadblocks to meeting strategic objectives.[10] To complicate matters, the interplay between various agencies' cyber-specific and general roles has generally been poorly considered, although there has been some improvement in this regard with the growing importance of – and therefore attention to – cybersecurity.

"Cybersecurity governance as a sum of individual parts" approach admittedly has its benefits. It evolves organically as society's digitalisation grows, and does not require fundamental reorientation in the tasks or governance areas of government agencies

This "cybersecurity governance as a sum of individual parts" approach admittedly has its benefits. It evolves organically as society's digitalisation grows, and does not require fundamental reorientation in the tasks or governance areas of government agencies. The straightforward individual mandates imply an imaginary promise of effectiveness: objectives and priorities can be set within a single domain, allowing problems to be limited to their own constituency, where one is less dependent on external commitment and resources. It is context-aware and hence better equipped to respond to sector-specific needs. On the other hand, it tends to overlook interconnectedness and cascading dependences, and there is a risk of conflicting activities and competition over the same limited resources.

2.2. Long-term vision and fundamental principles

Successfully developing national cybersecurity is a continuous process and, ideally, strategic planning periods should consciously contribute to both a short-term and a long-term view. Today's success builds on the work and decisions of previous strategy periods, while the connection to earlier efforts is not necessarily evident. This means, however, that measuring the success of each strategy period is somewhat artificial: establishing success on the building blocks set during earlier time frames shows visible results of amplified compound gain, while setting building blocks that can only be "cashed in" as successes during

[8] Alexander Klimburg (ed.), *National Cyber Security Framework Manual* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012), 94–101, https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf; International Telecommunication Union, World Bank, Commonwealth Secretariat,Commonwealth Telecommunications Organisation, and NATO Cooperative Cyber Defence Centre of Excellence, *Guide to Developing a National Cybersecurity Strategy – Strategic Engagement in Cybersecurity* (Geneva: The International Telecommunication Union, 2018), 36, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

[9] See the CCDCOE National Cybersecurity Organisation series, available at https://ccdcoe.org/library/publications/ and https://ccdcoe.org/library/strategy-and-governance/.

[10] Toomas Vaks, *Küberjulgeoleku strateegia mõju küberturvalisuse arengule Eestis 2008-2018* [The impact of cybersecurity strategy on the development of cybersecurity in Estonia in 2008–18] (Tallinn: Tallinna Tehnikaülikool, 2018), 52, https://digikogu.taltech.ee/en/Download/fb794e52-07fd-4b49-93cb-3be2c56d95c2.

Vision		
2008–2013	**2014–2017**	**2019–2022**
Reduced vulnerabilities of cyberspace in the nation as a whole[11]	Estonia is able to ensure national security and support the functioning of an open, inclusive and safe society	Estonia is the most resilient digital society
Fundamental principles		
2008–2013[12]	**2014–2017**	**2019–2022**
Cybersecurity action plans should be integrated into the routine processes of national security planning	Cybersecurity is an integral part of national security, supporting the functioning of the state and society, the competitiveness of the economy and innovation	We consider the protection and promotion of fundamental rights and freedoms as being as important in cyberspace as in the physical environment
Cybersecurity should be pursued through the coordinated efforts of all concerned stakeholders, of the public and private sectors as well as of civil society	Cybersecurity is ensured in a coordinated manner through cooperation between the public, private and third sectors, taking into account the interconnectedness and interdependence of existing infrastructure and services in cyberspace	We see cybersecurity as an enabler and amplifier of Estonia's rapid digital development, which is the basis for Estonia's socioeconomic growth. Security must support innovation and vice versa
Effective cooperation between the public and private sectors should be advanced for the protection of critical information infrastructure	Cybersecurity is ensured on the basis of the principle of proportionality while taking into account existing and potential risks and resources	We recognise the security assurance of cryptographic solutions to be of unique importance for Estonia as it is the foundation of our digital ecosystem
Every information system owner should be aware of his or her responsibilities in the prudent use of information systems and should also take the necessary security measures to manage identified risks	Cybersecurity starts with individual responsibility for safe use of ICT tools	We consider transparency and public trust to be fundamental for a digital society. We therefore commit to adhere of the principle of open communication
A general social awareness of threats in cyberspace and the state of readiness to meet them should be fostered	A top priority in ensuring cybersecurity is to anticipate and prevent potential threats and respond effectively to threats that materialise	
Estonia should cooperate closely with international organisations and other countries to increase cybersecurity globally	Cybersecurity is ensured via international cooperation with allies and partners. Through cooperation, Estonia promotes global cybersecurity and enhances its own competence	
Proper attention should be paid to the protection of human rights, personal data and identity	Cybersecurity is ensured by respecting fundamental rights and freedoms as well as by protecting individual liberties, personal information and identity	
The development and administration of IT solutions for the provision of public services should be brought into compliance with relevant frameworks and policies to ensure the continuity and recovery plans of their information systems	Cybersecurity is supported by intensive and internationally competitive research and development	

Table 1. Vision and fundamental principles of Estonian national cybersecurity strategies

[11] 'Vision' is not explicitly defined in the 2008 strategy and has been extracted from the text.

[12] Some detail has been omitted from a few entries without altering the meaning in order to keep the compact format of the overview table.

future strategy windows, without offering immediate benefit, is not reflected in this measurement.

Estonia's cybersecurity vision has consistently focused on protecting the digital society as a whole, while the fundamental principles have carried the idea of protecting and promoting fundamental rights in cyberspace, and Estonia's openness and contribution in international developments

The strategy's vision and fundamental principles should serve as soft balancing mechanisms to shift the focus away from optimising for short-term progress at the expense of building long-term success – which occurs when effort is concentrated on picking tactical victories, possible thanks to earlier investments, and leaving no resources for setting a path for a successful future (such as education, R&D and international contributions towards shaping the global digital environment).

Each of Estonia's three cyber strategy documents to date has outlined the overall strategic vision and a set of fundamental principles to embody the underlying value system for strategic planning. The vision and fundamental principles for each strategy period are summarised in Table 1.

Throughout all strategy periods, Estonia's cybersecurity vision has consistently focused on protecting the digital society as a whole, while the fundamental principles have carried, in various forms, the idea of protecting and promoting fundamental rights in cyberspace, and Estonia's openness and contribution in international developments. Both the vision and principles focus on building long-term value and contribute to Estonia's success that has enabled accomplishments in international alliances and cooperation formats, building e-services on a secure digital identity framework, and relying on the relatively high maturity of critical information infrastructure.

A consistent vision and fundamental principles support long-term strategic alignment and build-up of compound value in both domestic and international collaboration. The long-term ambition should be balanced with an agile openness to make adjustments at the highest level of strategic planning. While each change needs to be well-motivated, and the top-most vision and principles are less suited for experimenting with frequent changes than lower-level goals and action plans, several reasons may justify change:

- when suggested by an increased maturity level – yesterday's vision could be today's baseline;
- in the event of external technological developments or changes in the overall threat landscape;
- when justified by lessons learned;
- when the existing vision or fundamental principles are unfit for their purpose as an alignment and communication tool for stakeholders and the target audience.

A universal strategic planning challenge, irrespective of the country or sector, is the risk of limiting the significance of a strategy document to a nice piece of writing that contains all the right principles and ambitions but has very little practical effect

As its cybersecurity strategic planning has evolved, Estonia's vision and fundamental principles have followed these ideas – the needs and maturity were clearly very different in 2008 and 2019. For example, an aspect introduced only in 2019 was the security assurance of cryptographic solutions – mainly building on the case of the 2017 ROCA eID vulnerability crisis, which highlighted Estonia's digital ID as the cornerstone of its entire digital ecosystem.[13]

[13] Estonian Information System Authority, "ROCA Vulnerability and eID."

2.3. Actionable and realistic strategic objectives

A universal strategic planning challenge, irrespective of the country or sector, is the risk of limiting the significance of a strategy document to a nice piece of writing that contains all the right principles and ambitions but has very little practical effect. The main causes for this include:

- a mismatch with the action plan, where the completion of a planned set of actions does not adequately contribute to reaching the corresponding strategic goal;
- resource planning is weakly linked with the strategy process – a challenge intensified for domains with a decentralised governance model (Estonia's cyber-security governance throughout all three strategy periods is a good example);
- insufficient connection and integration with other national strategic planning documents – stand-alone efforts within an isolated cybersecurity strategy lead to weak results. With cybersecurity becoming an integral part of all fields of governance and policy planning at national level, this challenge will grow over time.

Two further underlying aspects can markedly reduce the practical applicability of a strategy: a lack of prioritisation and an insufficient or misleading performance measurement framework, which will be described in more detail below.

Indeed, Estonia's cybersecurity strategy practice has struggled with all of the above.[14] Expert interviews conducted in 2018 regarding Estonia's key cybersecurity strategy challenges cited failures in resource planning (recognising cybersecurity as a priority but failing to match this with resource allocation); a lack of connection with overall national strategic planning, where the Cybersecurity Strategy was treated as an isolated document with stakeholders failing to recognise responsibilities as theirs; plus interagency rivalries.[15]

2.3.1. A collective letter to Santa Claus – or, everything is important!

Nearly all strategic planning processes, irrespective of the field or nation, have limitations set by available human and financial resources. This is especially true for Estonia as a very small country, meaning that setting clear priorities is of defining importance.

Cybersecurity planning induces a strong initial intuition that everything is important, often amplified by stakeholders who each argue from the perspective of their own most burning issues

Cybersecurity planning induces a strong initial intuition that everything is important, often amplified by stakeholders who each argue from the perspective of their own most burning issues. As a result, unclear priorities – wanting it all and wanting it now – emerge, subsequently facing resource constraints. Ideally, the strategy process is designed so that this mismatch is identified and addressed during development. However, as this is an extremely difficult discussion – which of all the very important things shall we not do during the next strategy period? – this step is often dismissed, leading to a vague strategy and arbitrary prioritisation.

This has been among the hardest trials for Estonia's cybersecurity planning during all strategy periods. The new, 2021, draft strategy will attempt to address this shortcoming of its predecessors, prioritising the strengthening of (1) core infrastructure and (2) incident prevention and response capabilities, instead of trying to boil the ocean.[16]

[14] Piret Pernik concluded in a 2013 review that: there were insufficient links between strategic objectives and measures on the one hand and budgeting and resources on the other; there was a lack of coherence between the cybersecurity strategy and agencies' mandates and actual activities, and between the cybersecurity strategy and key state documents and government development plans; and the strategy duplicated other development plans. See Piret Pernik, *Küberjulgeoleku strateegia 2008–2013 analüüs* [Analysis of the cybersecurity strategy 2008–13] (Tallinn: Rahvusvaheline Kaitseuuringute Keskus, 2013), 5–6.

[15] Vaks, *Küberjulgeoleku strateegia mõju*, 29–30.

[16] Draft *Digital Society Development Plan 2030.*

2.3.2. Struggling with metrics

It is widely acknowledged that an actionable national cybersecurity strategy must be paired with quantifiable goals. According to the leading academic authorities in quality management studies, H. James Harrington and Thomas McNellis, "measurement is the first step that leads to control, and, eventually, to improvement. If you can't measure something, you can't understand it. If you can't understand it, you can't control it. If you can't control it, you can't improve it."[17] However, attaching measurable quantities to strategic goals may turn out to be the most challenging task in strategic planning. A metrics system can fail for several reasons: the design of the metrics may be misaligned with strategic priorities or insufficient to address them; or there may be underlying data quality issues, overly ambiguous metrics, or insufficient monitoring, reporting and follow-up. The fact that cybersecurity is a discipline undergoing intense development does not make the task easier: what constitutes an adequate maturity level remains a moving target.

Failures, in turn, transfer to overall weaknesses in strategic planning and efficient governance. Poor data quality and misaligned or inadequate design of the metrics system may lead to communicating arbitrary information or miscommunication of the status quo to decision-makers. This in turn can lead to reactive escalation and disproportionate attention to specific facets of the security landscape, while ignoring the remainder of the spectrum. Aspects that are not measured – due, for example, to lack of data or measurement maturity – may become increasingly neglected and, as inadequately aligned metrics, can encourage a false sense of security regarding success or failure.

Estonia has seen many of these shortcomings in its strategic planning periods, from a lack of metrics and irrelevant metrics to insufficient attention and monitoring. A desire for comprehensive progress monitoring led to the inclusion of performance indicators in the 2014 strategy, even if analysis preceding their formulation was scant and the indicators themselves often appeared token in nature rather than substantial. Of course, such challenges were hardly unique; according to the Global Cybersecurity Index (GCI) 2017, a mere 21% of countries globally included some form of performance metrics in their cybersecurity strategy, while the indicator had significantly improved to 47% by time of the subsequent report.[18] It can be expected that the capacity and maturity for cybersecurity performance monitoring will improve along with the increasing maturity of the discipline as a whole.

Viewing cybersecurity strategy as a process, rather than simply an outcome document, strengthens connections between the government agencies involved, and also with non-government stakeholders that represent an essential pillar of national cybersecurity

Estonia has seen many shortcomings in its strategic planning periods, from a lack of metrics and irrelevant metrics to insufficient attention and monitoring

2.4. National strategy as a process, not just a document

Estonia has, from the onset, followed the principle of inclusiveness in the strategy development process, recognising the need to engage a wide range of stakeholders in both the strategy planning and implementation

[17] H. James Harrington and Thomas McNellis, "Mobilizing the Right Lean Metrics for Success," *Quality Digest,* May 2006, https://www.qualitydigest.com/may06/articles/02_article.shtml.

[18] International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI) 2017* (Geneva: ITU-D, 2017), 27–37, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf; International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI) 2018* (Geneva: ITU-D, 2018), 18. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

phases.[19] This has to do with Estonia's established approach to public policy and administration, in which those impacted by a policy choice must be given a chance to voice their views, but also recognising the role of private-sector stakeholders as providers of essential services, and their unique knowledge and expertise.[20] Viewing cybersecurity strategy as a process, rather than simply an outcome document, strengthens connections between the government agencies involved, and also with non-government stakeholders that represent an essential pillar of national cybersecurity.

Bringing together all stakeholders and enabling interconnected dialogue on strategic directions and collaboration tools may in the end be more impactful than concluding an eloquent, academically sound document. In terms of producing sustained effect, a meaningful, engaged process has proved a deliverable in its own right: the process of producing Estonia's first cybersecurity strategy in 2008 was considered among its most important achievements as it brought together state institutions and strengthened the government's cooperation with private companies and educational institutions.[21] Experts interviewed for a 2018 study viewed the strategy preparation and implementation process as having strengthened Estonia's cybersecurity posture, as the effort created both a structure to address cyber issues and a platform for recognising key problems and identifying solutions in a concerted manner. There was an almost unanimous view that the process and outcome alike were key factors in achieving a systematic approach and gaining broad public and political recognition for cybersecurity as a matter of public and national security.[22] In addition, the strategy process helps uphold a broader public interest in finding solutions to the sector's challenges – which stimulates developments even beyond the objectives and measures directly addressed in the strategy text itself. [23]

Pursuing intense stakeholder involvement as a priority comes at a cost: it makes the document relatively expensive to produce and the process is lengthy and potentially chaotic. At the same time, academic quality might be lost compared to having a few strategic planning consultants putting the document together without "messy" discussions. One may be tempted to consider procuring a strategy from planning experts or copying from leading strategies around the world. However, the effort put into intense stakeholder management brings proportionate value in terms of community commitment. Despite the time and resource intensity of the preparation and implementation of strategies, it enables systematic management of the developments and is hence expedient from the point of view of the state, presumably not only in Estonia but also in other countries.[24]

The effort put into intense stakeholder management brings proportionate value in terms of community commitment

2.5. The strategy as a tool for international collaboration

The publication of cybersecurity strategies plays an important role in declaring national priorities and explaining them to stakeholders and partners, thereby defining and legitimising the presence and purposes of the public administration in this domain.[25] Beyond publishing them for the awareness of its domestic stakeholders, Estonia has tried to make all three of its cybersecurity strategy documents accessible online to a broad international audience, translating them into English. This provides a meaningful disclosure of the planned activities and a reasonable level of understanding of the underlying process.

[19] *Inclusiveness* is recognised as one of the nine overarching principles of strategic cybersecurity, acknowledging that the strategy should be developed with the active participation of all relevant stakeholders and should address their needs and responsibilities. See International Telecommunication Union et al, *Guide to Developing a National Cybersecurity Strategy,* 31.

[20] Pursuant to the Administrative Procedure Act, § 40. See Riigikogu, "Administrative Procedure Act," *Riigi Teataja* (State Gazette), RT I 2001, 58, 354 (27 March 2019) (translation), https://www.riigiteataja.ee/en/eli/527032019002/consolide. Similar provisions exist in sectoral acts, e.g. regulation of the telecommunications market, spatial planning.

[21] Pernik, *Küberjulgeoleku strateegia,* 29.

[22] Vaks, *Küberjulgeoleku strateegia mõju*, 49.

[23] Ibid., 53.

[24] Ibid.

[25] Ibid., 49.

The sharing of information by states on their national cybersecurity strategies is recognised as one of the confidence-building measures defined by the Organisation for Security and Cooperation in Europe (OSCE) in 2016.[26]

Such international transparency makes the strategy document a useful tool in communication with international counterparts for identifying the collaborative potential of dialogue partners, supporting global capacity-building efforts and, not least, upholding a country's standing as a trusted, open and valuable partner. Estonia considers its reputation as a capable partner and a clear voice in the international arena as an asset supporting the exchange of information and knowledge with strategic partners, thereby strengthening its strategic objectives and values.[27]

Conclusions

Studies confirm that both Estonia's cybersecurity strategies and the strategy development process as a whole have had a tangible, positive impact on Estonia's cybersecurity capacity development. Both cybersecurity as an outcome and the strategic planning process have been pursued as nationwide, multi-stakeholder processes in which the private sector and other stakeholders have been engaged.[28]

Estonia's successes and failures in developing and implementing national cybersecurity strategies point to several universally applicable aspects. Based on this experience, we have chosen to highlight the five most relevant deliverables, along with related challenges:

- **Defining a successful governance model.** The decentralised governance model pursued by Estonia has its benefits and challenges. While organisations' broad autonomy stimulates partnerships, the consistency of actions and efficient use of resources are difficult, requiring particular attention to the division of responsibilities, coordination, and mechanisms for decision-making;

- **Providing long-term vision and fundamental principles** to guide value-driven strategic development that remains consistent across strategy periods, yet is open to revision and adjustment where justified;

- **Setting actionable and realistic strategic objectives**, along with a comprehensive system of metrics that help to understand, control and improve performance, and ensuring the necessary focus and prioritisation;

- **Investing in cybersecurity strategy as a process** in order to ensure close involvement of stakeholder groups and a strong community, and resisting the temptation to merely settle for a presentable document;

- **Communicating national priorities** to international stakeholders and partners.

It is hoped that such candid discussion of the successes and failures of the national cybersecurity strategic planning experience will have practical educational value for those analysing their own success in implementing cybersecurity strategy and defining its future objectives and priorities, and revising the viability of long-term vision and principles.

There are undoubtedly many differences between Japan and Estonia: size, demographics and population density, economic structure, public administration and policy tradition, and history. Yet in terms of both the reliance of society on digital infrastructure, the significance of cybersecurity for societal resilience, and the vital importance of rules-based cyberspace and effective international cooperation and information sharing, they have plenty in common. Japan has been a prime dialogue partner for Estonia in the Asia-Pacific region, and the mutual sharing of information and lessons learned in the area of cybersecurity has benefited both parties. Given the value of such exchanges, we hope this chapter will contribute to their continuation on the strategic planning level, strengthening the cyber resilience of both countries.

[26] Organisation for Security and Co-operation in Europe (OSCE), "Decision No. 1202. OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies," *PC Journal*, No. 1092, 10 March 2016, https://www.osce.org/files/f/documents/d/a/227281.pdf.

[27] Ministry of Economic Affairs and Communications, *Cybersecurity Strategy 2019-2022,* Section 1.3 and Objective 3.

[28] Vaks, *Küberjulgeoleku strateegia mõju*, 53.

CHAPTER III

Aligning Estonian and Japanese Efforts in Building Norms in Cyberspace

Anna-Maria Osula

Introduction

The digital transformation of societies has expanded the attack surface, rendering malicious cyber activities a part of our everyday lives. According to some studies, cybercrime had cost the world €5.5 trillion by the end of 2020, up from €2.7 trillion in 2015, due in part to the exploitation of the Covid-19 pandemic by cybercriminals.[1] Alarmingly, the capabilities of cyber-threat actors are continuously advancing, with the attacks possibly inflicting serious damage or showcasing political motives, and thereby potentially threatening democratic processes such as elections.[2] Recent years have also witnessed increasing geopolitical concerns in areas such as connectivity, privacy and the free flow of information. Consequently, states are battling for a better position in both governing technologies and being at the forefront of technological innovation.

As a member of the European Union, Estonia broadly follows the rhetoric and direction of EU strategic objectives. With its new Cybersecurity Strategy, released in 2020, the EU confirms its ambition to be in the lead for the digital economy, to invest more in technology and to remain the frontrunner in maintaining a high level of protection for the whole of society.[3] Rules, regulations and norms have an important role to play in achieving this. Hence, the EU and Estonia continuously underline the applicability of international law and the importance of adhering to norms of state behaviour in cyberspace.

The EU and Estonia continuously underline the applicability of international law and the importance of adhering to norms of state behaviour in cyberspace

Japan is a key strategic partner for the EU in several important areas, cybersecurity being one of the domains identified for closer cooperation.[4] Japan has recently increased its focus on reinforcing cybersecurity both for public and private actors, keeping in mind the

[1] Igor Nai Fovino et al, *Cybersecurity, Our Digital Anchor* (Luxembourg: Publications Office of the European Union, 2020), 7, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC121051/cybersecurity_online.pdf.

[2] ENISA, *ENISA Threat Landscape - The Year in Review* (Attika: European Union Agency for Cyber Security, 2020), 8, https://www.enisa.europa.eu/publications/year-in-review/at_download/fullReport.

[3] European Commission High Representative of the Union for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade* (JOIN (2020)18 Final) (Brussels: European Commission, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN.

[4] Council of the European Union, "Enhanced EU Security Cooperation in and with Asia: Council Conclusions," 9265/1/18 REV 1, 28 May 2018, https://www.consilium.europa.eu/media/35456/st09265-re01-en18.pdf; European Commission, "Annex 3 of the Commission Implementing Decision on the 2019 Annual Action Programme for cooperation with third countries to be financed from the general budget of the European Union: Action Document for 'Security Cooperation in and with Asia'," 2019, https://ec.europa.eu/fpi/sites/fpi/files/annexe_3_security_cooperation_in_and_with_asia_part1_v2.pdf.

Tokyo 2020 Olympic and Paralympic Games that should take place in the summer of 2021. Equally, recent Japanese cybersecurity strategies have underlined the role of cyber diplomacy, international cooperation and their close relationship with Japan's national security, and Japan is an avid supporter of the free flow of data.[5]

In light of Japan being a strategic partner for the EU in the cybersecurity domain, this chapter looks specifically at the cooperation between Estonia and Japan. While cybersecurity-related cooperation between the two countries began cautiously, the chapter examines recent developments in aligning the two countries' positions regarding building and promoting norms of state behaviour in cyberspace. In order to understand Estonia's unique position and to establish small states as credible partners in cyber diplomacy negotiations, the chapter will first set the scene by outlining the potential of small states to play a substantial role in taking the discussions on norms of state behaviour forward in international and regional fora. The chapter will then identify points of agreement and key similarities between Estonian and Japanese perspectives and offer suggestions for further cooperation.

1. Small States and Building Cyber Norms

Four pillars – international law, norms of state behaviour, confidence building and capacity building – form the backbone of current UN-level discussions on building and maintaining trust and security in the digital environment. International law and voluntary, non-binding norms of responsible state behaviour play a crucial role in clarifying state responsibilities in cyberspace. While international law is the foundation of stability and predictability in relations between states, norms play an important role in reflecting the expectations of the international community, reducing risks of misperceptions, and thus contributing to the prevention of conflict.[6] According to commentators, cyber norms and international law remain the best and most reliable way to build international security in cyberspace.[7]

International law and voluntary, non-binding norms of responsible state behaviour play a crucial role in clarifying state responsibilities in cyberspace

In particular, adherence to international law plays an important role in protecting small nations that cannot boast great military power or significant resources. In the words of Lennart Meri, Estonia's first post-Cold War president, "international law is the nuclear weapon of a small state".[8] Commonly agreed international legal norms provide clarity that allows states to foresee with certainty what actions would be considered as violating international law. International law also offers options for legal remedies to be used in the event of an offensive cyber operation being launched against a state. It is the assumption that such legal predictability, combined with other legal factors such as investigative measures, sanctions and a functioning judicial system, also acts as a deterrent against possible attacks.

Adherence to international law plays an important role in protecting small nations that cannot boast great military power or significant resources

[5] See: Government of Japan, *Cybersecurity Strategy 2018* (Tokyo: NISC, 2018), https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf. The Japanese Prime Minister Shinzo Abe proposed the concept of Data Free Flow with Trust at the Davos Meeting in 2019 and reiterated it at the G20 and G7 summits. See: Ministry of Foreign Affairs of Japan, "Speech by Prime Minister Abe at the World Economic Forum Annual Meeting," 23 January 2019, https://www.mofa.go.jp/ecm/ec/page4e_000973.html.

[6] See generally the UN GGE reports of 2013 and 2015, and: United Nations Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, *Final Substantive Report* (A/AC.290/2021/CRP.2) (New York, NY: United Nations, 2021), https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

[7] James Lewis, "Overview of the Cyber Stability Framework: Norms of Responsible State Behaviour, International Law, Confidence and Capacity Building Measures," Tallinn Winter School of Cyber Diplomacy, 9–10 February 2021, https://vm.ee/et/node/53915.

[8] Lauri Mälksoo and Adam Lupel, "A Necessary Voice: Small States, International Law, and the UN Security Council," blog, ETH Zürich Center for Security Studies, 29 April 2019, https://css.ethz.ch/en/services/digital-library/articles/article.html.

However, this does not mean that small states necessarily exhibit a united position in defending the international legal order. In debates on state behaviour in cyberspace, small states are split by the same geopolitical fault lines as their bigger counterparts, and often disagree about the meaning and scope of application of international law. In the context of state behaviour in cyberspace, this can clearly be seen in the recent standoff at the United Nations, with Russia and the US proposing in 2018 two separate initiatives (respectively, the next iteration of the United Nations Group of Governmental Experts (UN GGE) and of the Open-Ended Working Group (OEWG)) to facilitate these discussions. While the UN General Assembly approved both proposals, the voting reflected the two opposing camps, largely falling along the lines of military and political alliances.[9] These two different groups also correspond to some of the debates over international law, such as the applicability of international humanitarian law to cyberspace. Despite the different views small states may have, the promotion of and commitment to the international rule of law is generally a common feature of their foreign policies and rhetoric.[10]

In debates on state behaviour in cyberspace, small states are split by the same geopolitical fault lines as their bigger counterparts

Expertise and skilful diplomacy, developed in niche areas over time, can be used to achieve small states' strategic objectives

Despite realpolitik arguments that powerful countries have more leverage in global politics, small states can prove effective in a number of ways. For example, their small size allows them to manoeuvre more quickly in policy debates, or adapt to technological change and innovation, without the constraints of large and static bureaucracies. In addition, when (human) resources are scarce, it makes sense to specialise on a strategic policy domain, build reputation and cultivate recognised expertise. This expertise and skilful diplomacy, developed in niche areas over time, can be used to achieve small states' strategic objectives as well as to provide "an important, credible voice with moral authority to remind all member states of their obligations under international law, reaffirm normative commitments to compliance, and advocate for a recommitment to a multilateral, rule-based order that is of collective benefit to the entire world".[11] Thereby, while small states may be subject to significant limitations in terms of resources and structural constraints (e.g. not being permanent members of the United Nations Security Council (UNSC)), it can be argued that they are nevertheless well positioned to play a modest though normatively critical role in defending international law.[12]

Cooperation and multilateral venues are of high importance to small states, who may use their strong position in such fora to feed into bilateral relationships

Cooperation and multilateral venues are of high importance to small states, who may use their strong position in such fora to feed into bilateral relationships. However, in order to have an influence on the decisions of larger state actors, small states need to earn their counterparts' trust, prove to be stable and credible partners, and demonstrate solid diplomatic skills. In fact, politicians and diplomats from small states have the potential to establish a neutral standing and thereby serve as remarkably successful mediators, primarily by mastering the skill of searching for compromise.[13] On the

[9] United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the First Committee" (A/73/505), Seventy-third session, Agenda item 96, 19 November 2018, https://undocs.org/A/73/505; Ilona Stadnik, "Discussing State Behaviour in Cyberspace: What Should We Expect?" DiploFoundation, 20 March 2019, https://www.diplomacy.edu/blog/discussing-state-behaviour-cyberspace-what-should-we-expect.

[10] Mälksoo and Lupel, "A Necessary Voice".

[11] Mälksoo and Lupel, "A Necessary Voice".

[12] Mälksoo and Lupel, "A Necessary Voice".

[13] Liina Areng, *Lilliputian States in Digital Affairs and Cyber Security* (Tallinn Paper No. 4) (Tallinn: NATO CCDCOE, 2014), 4, https://ccdcoe.org/uploads/2018/10/TP_04.pdf.

other hand, small states are often reliant on like-minded coalitions or security alliances, and thereby may not be perceived as truly neutral in situations of clearly opposing debates.[14]

Small states may also successfully act as norm entrepreneurs. According to Martha Finnemore and Duncan Hollis, norms may arise in many ways:

> They may emerge spontaneously or through the entrepreneurship of one or more actors who frame the issue, articulate the norm, and organize support. If such efforts are successful, the norm may reach a tipping point and cause a "cascade" of norm adoption or, in other cases, cycles of norm change. Norm promoters draw on a variety of tools to construct the norm and create support for it, including incentives, persuasion, and socialization.[15]

Accordingly, norm entrepreneurs may be organisations, companies, individuals and states. They are critical to establishing a norm not only because they call attention to an issue in general but because they frame it. This entails employing language that names, interprets and dramatises the problem, and on that basis proposes a norm to address it, often also providing for an organisational platform.[16] And even if not qualifying as a norm entrepreneur as outlined by Martha Finnemore and Kathryn Sikkink's original research, studies have shown that, for small states with big ideas, the promotion of norms can be a powerful means to further national interests on the global level.[17]

2. Estonia as a Norm Promoter in Cybersecurity

As a digitally highly advanced society, Estonia has been at the forefront of discussions on cybersecurity since it was the target of the world's first coordinated cyber-attack campaign against a nation-state in 2007. This incident gave a boost to conceptualising cybersecurity on a domestic level (such as adopting the first cybersecurity strategy in 2008) as well as bringing the topic of cyber threats and the role of international cooperation in responding to such attacks to the agendas of international organisations such as NATO. Today, Estonia ranks high in global cybersecurity, Internet freedom and e-governance indexes.[18] The country also hosts relevant international organisations, such as the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE, also the birthplace of the Tallinn Manual, and a number of globally well-known cyber exercises such as Locked Shields) and the EU Agency for Large-Scale IT Systems, and seeks to offer an innovative and supportive environment to start-ups and technology companies.

Estonia has played an important role in building and promoting cyber norms in international and regional fora

Estonia has played an important role in building and promoting cyber norms in international and regional fora. It has been an active member of the UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security in 2009–10, 2012–13, 2014–15, 2016–17 and 2019–21. Importantly, the UN GGE's landmark consensus report in 2013 affirmed the application of

[14] Liisi Adamson, "Let Them Roar: Small States as Cyber Norm Entrepreneurs," *European Foreign Affairs Review* 24, no. 2 (May 2019): 222, https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/24.2/EERR2019014.

[15] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110, no. 3 (July 2016): 445, https://doi.org/10.1017/S0002930000016894.

[16] Finnemore and Hollis, "Constructing Norms," 447–48.

[17] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 887–917; Matthew Crandall and Collin Allan, "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms," *Contemporary Security Policy* 36, no. 2 (May 2015): 346–68, https://doi.org/10.1080/13523260.2015.1061765.

[18] "NCSI: Ranking," e-Governance Academy Foundation, accessed 7 February 2021, https://ncsi.ega.ee/ncsi-index/; Freedom House, *Freedom on the Net 2020: The Pandemic's Digital Shadow* (Washington, DC: Freedom House, 2020) https://freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf; United Nations Department of Economic and Social Affairs, *United Nations E-Government Survey: Digital Government in the Decade of Action for Sustainable Development* (New York, NY: United Nations, 2020), https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf.

international law in cyberspace, and the 2015 report proposed 11 norms for behaviour by states in cyberspace. In 2019–21 Estonia is also a member of the UN OEWG. While both the UN GGE and the OEWG are political discussions and not law-making processes per se, they have a significant role to play in shaping and establishing international agreement on norms of behaviour in cyberspace. In addition to global platforms, Estonia values the role of regional organisations in building trust and confidence between states and enforcing agreed norms.[19]

Estonia and other co-hosting countries put cybersecurity on the agenda of the UNSC, which had never before discussed the subject

As a major contribution, Estonia and other co-hosting countries put cybersecurity on the agenda of the UNSC, which had never before discussed the subject. As part of Estonia's Presidency of the UNSC, it organised an Arria-formula meeting focusing on cyber stability, conflict prevention and capacity building. Around 60 countries and organisations took part, many stressing the application of international law in cyberspace and underlining that norms of responsible state behaviour hold for all UN member states.[20] In addition, Estonia, supported by the UK and the US, raised the issue of responsible state behaviour in cyberspace in the UNSC and issued a joint stakeout condemning a large-scale cyber-attack conducted by Russia's military intelligence service against the government and media websites in Georgia in October 2019.[21]

These steps illustrated how active participation in international organisations allows small nations to bring urgent issues such as cybersecurity into the global limelight.

As a concrete step towards more clarity over the interpretation of international law, Estonia delivered its views on the issue in 2019. President Kersti Kaljulaid underlined in her speech the protection provided by international law to small states, stating that Estonia did not have "the luxury" of remaining unambiguous about the meaning of legal norms in cyberspace, and invited other nations to call out cyber operations that constitute a violation of international law.[22] The Estonian position includes several important points on due diligence and the right to resort to countermeasures. While its stance did not entail a clarification on the issue of whether sovereignty is a stand-alone rule or principle in international law, Estonia made a bold statement on collective response to malicious cyber activities, stating that "states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation". It was the first country in the world to offer such an interpretation of international law.[23]

Estonia made a bold statement on collective response to malicious cyber activities, stating that "states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation". It was the first country in the world to offer such an interpretation of international law

While the majority of other countries have not expressed their opinion about collective countermeasures, the proposal has certainly

[19] Permanent Mission of Estonia to the UN, "Opening Statement by the Republic of Estonia, by Amb. Heli Tiirmaa-Klaar for the UN GGE Panel on Regional Consultations," 2019, https://www.un.org/disarmament/wp-content/uploads/2019/12/estonia-gge-panel-on-regional-consultations-05-12-2019.pdf.

[20] Permanent Mission of Estonia to the UN, "At Estonia's Initiative, the International Community Reaffirmed the Importance of Cyber Stability, Including during the COVID-19 Crisis, at the UN Security Council," 23 May 2020, https://un.mfa.ee/at-estonias-initiative-the-international-community-reaffirmed-the-importance-of-cyber-stability-including-during-the-covid-19-crisis-at-the-un-security-council/.

[21] Permanent Mission of Estonia to the UN, "Stakeout on Cyber-Attack against Georgia by Estonia, the United Kingdom and the United States," 5 March 2020, https://un.mfa.ee/press-stakeout-by-estonia-the-united-kingdom-and-the-united-states-on-cyber-attack-against-georgia/.

[22] Office of the President of Estonia, "Speech of the President of the Republic of Estonia at the Opening of CyCon 2019," 29 May 2019, https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html.

[23] Michael Schmitt, "Estonia Speaks Out on Key Rules for Cyberspace," Just Security, 10 June 2019, https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/.

drawn attention to the need to review states' options for responding to malicious cyber activities. Moreover, the proposal signals to wrong-doers that the consequences of attacking a small state need not be limited to that state's own capabilities. So far, France has rejected the concept of collective countermeasures, while New Zealand acknowledges their possible use in assisting victim states in applying proportionate countermeasures to induce compliance by the state acting in breach of international law.[24] If Estonia decides to promote this norm internationally by framing the issue, further articulating the need and reasoning, and organises support from other countries, it could be seen as a norm entrepreneur as prescribed by Finnemore and Sikkink.

Also relevant is Estonia's role in raising awareness and providing training on different aspects of state behaviour in cyberspace. In addition to the wide range of training provided by the NATO CCDCOE, the Estonian Ministry of Foreign Affairs has organised high-level summer and winter schools for diplomats across the world. Equally, the Estonian Information System Authority is the coordinating body for the EU-wide network of cybersecurity experts CyberNet and a partner of the EU's Cyber for Development Project (Cyber4Dev), which aims to support the enhancement of cybersecurity in Africa, Asia, Latin America and the Caribbean through various training programmes. [25]

Given the above, it is fair to conclude that Estonia's continuous activity targeting different facets of cybersecurity and norms for responsible state behaviour, promoting cyber stability and cooperation, and acting as a trustworthy partner and trainer, has over time cultivated for the small country a reputation for consistency and credibility in the domain of cybersecurity and norms of state behaviour in cyberspace.

3. Estonia and Japan Fostering Cooperation in Cybersecurity

Estonia and Japan have many similarities in their approach to state behaviour in cyberspace, which has established firm ground for closer bilateral ties. Both face complicated geopolitical challenges and both are active members in international and regional organisations dealing with norms in cyberspace. As leaders in cyber diplomacy, they frequently speak out on the applicability of international law to cyberspace, and express concerns about states carrying out malicious cyber operations. Importantly, Estonia and Japan play an active part in negotiations in the UN GGE and OEWG, where their main positions largely converge. These include: (1) views on the applicability of international law, (2) the lack of a need for a new legally binding instrument on cybersecurity, (3) relevance on implementation of already agreed norms, and (4) the centrality of confidence and capacity building. While Estonia has submitted its views for inclusion in an annex to UN GGE reports on one occasion (in 2017), Japan has been more active and shared its domestic views three times (in 2016, 2017 and 2019).[26]

Estonia and Japan have many similarities in their approach to state behaviour in cyberspace, which has established firm ground for closer bilateral ties

[24] Ministère des Armées (Ministry of Armed Forces), *Droit International Appliqué Aux Opérations Dans Le Cyberspace* [International Law Applied to Cyberspace Operations] (Paris: Délégation à l'information et à la communication de la défense, 2019), 8, https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf; Ministry of Foreign Affairs and Trade of New Zealand, "The Application of International Law to State Activity in Cyberspace," 1 December 2020, para. 22, https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf.

[25] "EU CyberNet – the bridge to cybersecurity expertise in the European Union," EU CyberNet, last accessed 18 February 2021, https://www.eucybernet.eu/; "We are Cyber 4 Dev," Cyber4DEV, last accessed 18 February 2021, https://cyber4dev.eu/.

[26] United Nations Office for Disarmament Affairs, "2017 Submissions from Member States: Estonia – Response to the General Assembly Resolution 70/237 on 'Developments in the Field of Information and Telecommunications in the Context of International Security'," 2017, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2017/09/Estonia-full.pdf; United Nations Office for Disarmament Affairs, "2016 Submissions from Member States: Japan," 2016, https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/10/Japan.pdf; United Nations Office for Disarmament Affairs, "2017 Submissions from Member States: Japan,"2017, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2017/09/Japan.pdf; United Nations Office for Disarmament Affairs, "2019 Submissions from Member States: National Reply from Japan," 2019, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/Japan-2019.pdf.

The alignment of values and principles between the two countries can also be seen in a number of other initiatives. For example, Estonia and Japan joined the statement on advancing responsible state behaviour, which promises to hold states accountable for actions breaching international law.[27] Estonia and Japan are also both signatories of the recent proposal for the Programme of Action to Advance Responsible State Behaviour in Cyberspace, which focuses on continuing institutional dialogue within the UN and moving forward with implementing the already agreed norms.[28] In addition, the two countries' support for each other's endeavours was outlined in a speech by the UN High Representative for Disarmament, Izumi Nakamitsu, delivered at the opening of a cyber event organised by Estonia in the margins of the UNSC.[29] It is also noteworthy that Estonia and Japan are among the signatories of the Council of Europe Convention on Cybercrime, and thereby actively promoting the expansion of its parties, strengthening international cooperation among law-enforcement authorities, assuring prompt and effective assistance in investigation, and facilitating international investigations.

On an institutional level, the two countries have cooperated over various aspects of cybersecurity since 2014, having signed a Memorandum of Understanding in 2015. Bilaterally, national views and best practices have been exchanged on a number of issues regarding technical capabilities, training and domestic frameworks. Japan contributed to the NATO CCDCOE as an observer in 2015–18 and joined as a Contributing Participant in 2019.

Both countries should continue efforts to raise awareness on responsible state behaviour in cyberspace

Conclusions

In future work, it is hoped that Estonia and Japan will identify further options for practical cooperation within the domain of cyber norms, and continue to develop their collaboration in technical, training, policy and other areas. Specifically, both countries should continue efforts to raise awareness on responsible state behaviour in cyberspace. General capacity building and information sharing on international law and its characteristics will be essential to reach a wider agreement on a number of issues related to norms. These include: (1) the long-lasting debate on the need for new norms as opposed to focusing on the implementation of existing ones, (2) different views on balancing sovereign rights and international commitments, and (3) the applicability of international humanitarian law to the militarisation of cyberspace.

Estonia and Japan should continue to identify and share their domestic views, legal assessments and experience related to cybersecurity

Equally, Estonia and Japan should continue to identify and share their domestic views, legal assessments and experience related to cybersecurity. Sharing information on the threat landscape and experience in mitigating cyber incidents will also be highly beneficial. As role models, the countries have the potential to influence other states in their respective regions to be more transparent regarding state practice and cooperation in terms of finding common ground in discussing norms, and in collaboration of a more technical nature.

[27] US Department of State Office of the Coordinator for Cyber Issues, "Joint Statement on Advancing Responsible State Behavior in Cyberspace," 23 September 2019, https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

[28] United Nations Office for Disarmament Affairs, "The Future of Discussions on ICTs and Cyberspace at the UN (Submission by France, Egypt, Argentina, Colombia, Ecuador, Gabon, Georgia, Japan, Morocco, Norway, Salvador, Singapore, the Republic of Korea, the Republic of Moldova, The Republic of North Macedonia, the United Kingdom, the EU and its member States – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, France, Finland, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden)," 8 October 2020, https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf.

[29] United Nations Office for Disarmament Affairs, "Briefing at the Security Council Virtual Arria-Formula Meeting on 'Cyber Stability, Conflict Prevention and Capacity Building': Remarks by Ms. Izumi Nakamitsu, High Representative for Disarmament Affairs," 22 May 2020, https://front.un-arm.org/wp-content/uploads/2020/05/UNSC-Arria-Formula-Meeting-on-Cybersecurity-HR-Remarks-22-May-2020.pdf.

As active members of regional organisations such as the EU and Asia-Pacific Economic Cooperation (APEC), Estonia and Japan also have the opportunity to guide discussion and serve as the voice of their closest neighbours and partners. For example, the EU is already taking concrete steps in finding a common voice for its 27 members by proposing to develop a joint position on the application of international law in cyberspace.[30]

Estonia and Japan may be far apart in geographical terms, but they are close in their understanding of the role, scope and objective of building norms in cyberspace

Estonia and Japan may be far apart in geographical terms, but they are close in their understanding of the role, scope and objective of building norms in cyberspace. The constructive cooperation and broad agreement on the future of the institutional setting for facilitating the international discussion on norms, international law, confidence building and capacity building are proof of common values. The close relationship between Estonia and Japan serves as an example of how the small size and population of a country has no effect on its credibility as an ally in promoting and developing norms of state behaviour in cyberspace.

[30] European Commission, *The EU's Cybersecurity Strategy for the Digital Decade*.

CHAPTER IV

Challenges and Next Steps for the Global CSIRT Community

Koichiro Komiyama

Introduction

Covid-19 has once again highlighted the importance of cyberspace. More than just a means of people's daily communication, it is the foundation of almost all economic activity and a new military domain of operations.

Exploring the mechanisms of effective governance and management of cyberspace is in the process of development. As pointed out in previous studies on international cybersecurity, the offensive side possesses a significant advantage, as there is no central control mechanism, no universally agreed definition of cyber warfare and no clear authority to enforce the rules.[1] Furthermore, there is no established and effective forum for global cybersecurity governance. Described as a "regime complex", the multilateral fora are disorganised and duplicative.[2]

Even in the absence of effective global governance, there are many cyber incident responders globally – operating for the private sector, government or academia – to help mitigate this situation. The global CSIRT (Computer Security Incident Response Team) community plays a crucial role in responding to cyber incidents.

This chapter focuses on relevant developments concerning the CSIRT community to discuss the future of global cybersecurity governance. The chapter first identifies and defines CSIRTs by providing context on their historical development and existing conceptual approaches. It then highlights core aspects that negatively affect international cooperation among CSIRTs, and ends with concluding remarks on the future development of CSIRTs together with thoughts on Estonian and Japanese cooperation in this domain.

Even in the absence of effective global governance, there are many cyber incident responders globally – operating for the private sector, government or academia

1. Preliminary Studies on CSIRTs

Existing research on CSIRTs can be roughly divided into two categories. On the one hand, there are materials describing the concepts and roles published by different CSIRTs or their community organisations. The handbook put together by the founders of CERT/CC, the world's first

[1] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (Kindle Ed.) (Oxford: Oxford University Press, 2017), 7; Mark Raymond, "Managing Decentralised Cyber Governance: The Responsibility to Troubleshoot," *Strategic Studies Quarterly* 10 (4), 2016, 123–49.

[2] Joseph S. Nye, "The Regime Complex for Managing Global Cyber Activities," *Center for International Governance and Innovation (CIGI) Publications* (1) (2014): 1–15.

What are CSIRTs?
[CSIRTs are] the fire brigade of the Internet.[6]
[CSIRTs are] key actors in the cyber regime complex that help the broader Internet community prevent and respond to cyber incidents through incident analysis and response, information sharing and dissemination, and skills training.[7]
[CSIRTs] embody the idea of science diplomacy through a self-organised professional culture with established information-sharing and monitoring practices, and recognised rules of engagement.[8]

Table 1. Definitions of CSIRTs

CSIRT, is a typical example.[3] FIRST (Forum of Incident Response and Security Teams), the world's largest CSIRT organisation, has also documented the roles required of a modern CSIRT.[4] However, these documents are more like manuals for engineers on how to run a CSIRT than comprehensive political science studies.

On the other hand, around 2014, CSIRTs began to attract the attention of researchers in international relations and security theory.[5] These studies have provided policymakers, the intended audience, with answers to a simple question: "What is a CSIRT?". Through these two quite different approaches, CSIRTs have been repeatedly defined.

1.1. Definitions

It is 30 years since the world's first CSIRT was created. Numerous CSIRTs exist globally, and the CSIRT community acts as a platform for these organisations to exchange information. Based on the studies referenced above, Table 1 summarises the most typical definitions of CSIRTs.

CSIRTs are becoming more and more subdivided in terms of their role, mandate and organisational structure. There are, for example, private CSIRTs that handle incidents for companies and organisations, national CSIRTs that serve as a national point of contact, regional CSIRTs for fostering regional collaboration, and PSIRTs that focus on the security of their products and users.[9]

The diversity of definitions is in itself an important key to understanding CSIRTs that originate from the practice of engineers who aim to resolve security incidents. As cybersecurity threats change from day to day, so does the role of CSIRTs.

[3] Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek, *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2nd Ed.) (Pittsburgh, PA: Carnegie Mellon Software Engineering Institute, 2003), https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf.

[4] FIRST, "Computer Security Incident Response Team (CSIRT) Services Framework (Version 2.1)," November 2019, https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf.

[5] Samantha Bradshaw, "Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity," Global Commission on Internet Governance Paper Series No. 23, Centre for International Governance Innovation and the Royal Institute of International Affairs (Chatham House), December 2015, https://www.cigionline.org/sites/default/files/gcig_no23web_0.pdf; Robert Morgus, Isabel Skierka, Mirko Hohmann, and Tim Maurer, *National CSIRTs and Their Role in Computer Security Incident Response* (Washington, DC: New America and Global Public Policy Institute, 2015), https://static.newamerica.org/attachments/11916-national-csirts-and-their-role-in-computer-security-incident-response/CSIRTs-incident-response_2-2016.eea78f5a4748443d8000903e300d5809.pdf; Isabel Skierka, Robert Morgus, Mirko Hohmann, and Tim Maurer, "CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams," Working Paper, Global Public Policy Institute & New America, May 2015, https://static.newamerica.org/attachments/2943-csirt-basics-for-policy-makers/CSIRT%20Basics%20for%20Policy-Makers%20May%202015%20WEB%2009-15.16efa7bcc9e54fe299ba3447a5b7d41e.pdf.

[6] "National Cyber Security Strategies – Interactive Map," ENISA, last accessed 26 March 2021, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

[7] Bradshaw, "Combatting Cyber Threats," 5.

[8] Leonie Maria Tanczer, Irina Brass, and Madeline Carr, "CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy," *Global Policy* 9 (November 2018): 60–66.

[9] For various types of CSIRTs, see also Skierka et al, "CSIRT Basics for Policy-Makers," 11–12. For PSIRTs, the framework document published by FIRST is a good reference – see FIRST, "Product Security Incident Response Team (PSIRT) Services Framework (Version 1.1)," Spring 2020, https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1.pdf.

1.2. Historical context

1.2.1. Birth of CSIRTs in the early days of the Internet

CSIRTs first came to the attention of international policy in 2015, when a report by the UN GGE, adopted unanimously by the UN General Assembly, set out norms for responsible state behaviour in cyberspace. The report also featured a norm to limit harmful activities against national CSIRTs, while prohibiting CSIRTs from undertaking malicious international activity.[10] It is clear that CSIRTs have gained a certain status in today's international community.

It is noteworthy that, although there is a globally accepted norm prohibiting attacks on CSIRTs, there is no common understanding of what CSIRTs are. And without proper knowledge of them, their role in future cybersecurity governance cannot be discussed. It is therefore useful to provide a short history of CSIRTs.

The first CSIRT was established on 17 November 1988.[11] A graduate student in the US developed and released a malware that took advantage of a known vulnerability in a mail server. Very swiftly, 10% of the 60,000 or so servers connected to the network at the time ceased to function. Shortly after the incident, the US Department of Defense and other relevant stakeholders held a meeting and identified the need for an organisation to share incident information and provide technical assistance in the future: the Computer Emergency Response Team Coordination Centre (CERT/CC) was established.

Later, similar organisations were created not only in the US but also in Europe and Asia. For example, SURFnet, the CSIRT of the Dutch researchers' network, was set up in 1992 and DFN-CERT was set up by a German academic institution in 1993. The Australian Researchers Network set up AusCERT in 2003, based at the University of Queensland. In the late 1990s, government-sponsored CSIRTs were established in the Asia-Pacific region, including Japan, South Korea and Singapore.

1.2.2. The need for international cooperation and scientific knowledge

As the name suggests, the CSIRT community is required to respond to incidents. There are two critical issues for effective response: (1) the need for operational international cooperation and (2) generating and sharing scientific knowledge, which is the main difference between CSIRTs and other organisations operating for law enforcement, intelligence agencies or the military.

The less geographically restricted nature of the Internet meant that international cooperation was essential for incident response

The less geographically restricted nature of the Internet meant that international cooperation was essential for incident response. In 1990, two years after the establishment of CERT/CC, a global community of CSIRTs called the Forum of Incident Response and Security Teams (FIRST) – founded by CSIRTs from France, other European countries and the US – began work. At the time of writing (March 2021), 562 CSIRTs from 97 countries are members of this global community. As Figure 1 illustrates, in less than 30 years, the CSIRT community has spread around the world, and regional CSIRT communities have been formed.[12]

Unlike police and intelligence agencies, in the 1990s many CSIRTs did not have explicit authority backed by national legislation or international agreements. In the absence of clearly defined procedures and roles, the international CSIRT community relied on the sharing of scientific knowledge as a framework for cooperation. A focus on scientific cooperation was essential to exchange and

[10] United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *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, NY: United Nations, 2015), https://undocs.org/pdf?symbol=en/A/70/174.

[11] Skierka et al, "CSIRT Basics for Policy-Makers," 7.

[12] APCERT in Asia, AfricaCERT in Africa, OIC-CERT in the Islamic Middle East, PacSON in the Pacific Island countries and ASEAN-CERT in the ASEAN member states are examples of regional communities.

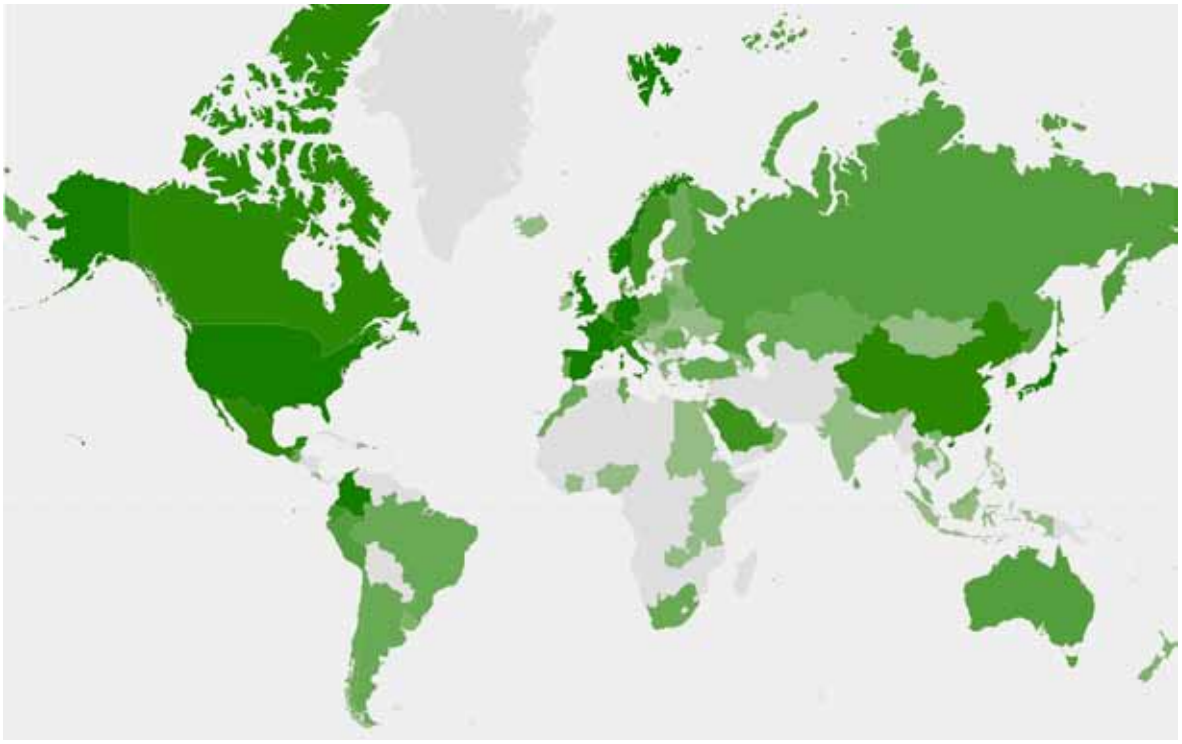

Figure 1. FIRST members around the world

Countries with CSIRTs which are members of FIRST are coloured in green. The darker the green, the greater the number of CSIRTs in each country that are members of FIRST. Source: First.org.

analyse operational incident information (e.g. relevant logs) to achieve better situational awareness and be able to mitigate incidents.

Since the early 2000s, the CSIRT community has been growing rapidly, requiring additional documentation on roles and functions. For example, West-Brown et al were pioneers in the field by articulating key principles of CSIRTs that are applied to this day, such as the need for defined constituents and providing a single point of contact.[13]

Looking back at the development of the CSIRT community from the perspective of global governance, it can be described as a process of transformation from a group of technicians responding to incidents out of necessity to a regime that performs a common task of responding to incidents based on common beliefs and scientific knowledge. It can also be seen as a transformation process from a state of incident response driven by common beliefs and scientific knowledge to a regime of incident response as a common enterprise.

[13] West-Brown et al, *Handbook.*

2. Reasons for Stalled International Cooperation

This section argues that, among the activities of CSIRTs, cooperation across national boundaries is on the wane and will become more intractable in the future. Four major problems are identified: (1) the nationalisation of cybersecurity, (2) the growing customisation of attacks, (3) commercialisation, and (4) national CSIRTs becoming governmental organisations.

From the early 2010s, there has been a growing recognition that cybersecurity is an integral part of ensuring national security, and also that the cyber domain can serve to project national power abroad

2.1. Nationalisation of Cybersecurity

From its birth, there was little doubt about recognising cyberspace as a global commons,

and the threats within it are therefore inherently transnational.[14] However, from the early 2010s, there has been a growing recognition that cybersecurity is an integral part of ensuring national security, and also that the cyber domain can serve to project national power abroad – including through offensive cyber operations. Twenty-one countries officially acknowledge offensive cyber capabilities, and another 24 are suspected of having them.[15] The practice of state-sponsored cyber-attacks harms international cooperation between CSIRTs.

As cybersecurity has become part of national security agendas, many have adopted the position that vulnerability information must be used to secure the home nation only, and not the global cyberspace

Some CSIRTs – including the CERT/CC in the US – perform Vulnerability Information Handling and are expected to warn affected users once a critical vulnerability is found. This is why, in 2018, the CERT/CC shared information when researchers at Google found a vulnerability in the Intel Central Processing Unit (CPU). Shortly afterwards, a US Senate committee criticised the CERT/CC for sharing vulnerability information with anyone outside the US, particularly referring to China.[16] As cybersecurity has become part of national security agendas, many have adopted the position that vulnerability information must be used to secure the home nation only, and not the global cyberspace. This trend clearly hinders information sharing between CSIRTs in different countries.

It is also becoming increasingly difficult for global CSIRT organisations to maintain their intended role due to national security considerations. In August 2019, for example, the US Export Administration Regulations were amended to prohibit "technology transfer" from US companies and organisations to certain Chinese companies, including Huawei.[17] As a result, and as a global organisation incorporated in the US, FIRST temporarily suspended Huawei's membership in order to avoid the risk.[18] In October 2019, Dahua Technology and Hikvision, manufacturers of video systems, were also suspended from membership of FIRST.

Developments related to the PacCERT case also represent a typical example of the trend that information sharing and regional cooperation among even neighbouring countries is becoming harder.[19] PacCERT is a regional organisation intended to provide cybersecurity incident response to 22 island countries in the South Pacific. Ministers of communications of these island nations agreed to establish a CSIRT in Fiji that would provide services to all of them.[20] A major driver of this was the economic rationale: instead of individual countries creating their own CSIRTs, they could take advantage of shared resources. Japan covered the initial cost through its Official Development Assistance (ODA) programme, expecting the island countries to share the operational costs after its launch.

Many experts visited Fiji to build facilities, purchase and set up equipment, and train staff.

[14] Many countries officially acknowledge cyberspace as a commons, and refrain from claiming sovereignty. The Government of Canada, for instance, declared that "Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship." Government of Canada, *Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada* (Ottawa: Government of Canada, 2010), 2, http://docshare01.docshare.tips/files/4043/40432912.pdf.

[15] "UN GGE and OEWG," GIP Digital Watch, last accessed 26 March 2021, https://dig.watch/processes/ungge.

[16] US Senate Committee On Commerce Science and Transportation, "Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown," hearings, 11 July 2018, https://www.commerce.senate.gov/2018/7/complex-cybersecurity-vulnerabilities-lessons-learned-from-spectre-and-meltdown.

[17] US Department of Commerce Bureau of Industry and Security, "Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List, effective August 19, 2019," 84 FR 43493, Federal Register Notices 2019, 21 August 2019, https://www.bis.doc.gov/index.php/federal-register-notices/17-regulations/1541-federal-register-notices-2019#fr54002.

[18] FIRST, "Statement Regarding Huawei's Suspension from the Forum of Incident Response and Security Teams (FIRST)," 18 September 2019, https://www.first.org/newsroom/releases/20190918.

[19] From 2010–2015, the author of this paper engaged in capacity building projects for PacCERT.

[20] Secretariat of the Pacific Community, "Pacific Regional ICT Ministers' Meeting 2010: Information and communication technology for development, governance and sustainable livelihoods of Pacific communities," *e-talanoa,* Issue 1 (2010): 2, https://www.jica.go.jp/project/fiji/002/materials/pdf/e_talanoa_issue_01_01.pdf; PacCERT Working Group, "Pacific CERT (PacCERT)," presentation, n.d., https://www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/docs/Pacific%20CERT%20(PacCERT).pptx.

As a result, PacCERT was established in 2012.[21] In 2014, however, the operation ceased due to financial problems. Although the ministers had agreed on sharing operational costs, the agreement was not implemented. It is easy to attribute the lack of success of PacCERT to financial difficulties, but it is also notable that some of the island nations have since invested significantly in cybersecurity.[22] Around 2013, countries such as Fiji, Papua New Guinea and Tonga began to prepare their own national CSIRTs. Island countries no longer faced the lack of funds and could afford to place higher priority on ensuring their own national security than on regional cooperation. As a result of this shift, PacCERT ceased to exist.

One of the core missions of CSIRTs has been to share technical security solutions as quickly as possible to mitigate the effects of cyber incidents

2.2. Growing Customisation of Attacks

One of the core missions of CSIRTs has been to share technical security solutions as quickly as possible to mitigate the effects of cyber incidents. After two decades of attackers and defenders competing with each other and developing their techniques, many defenders adopted so-called techno-regulation strategies by designing certain barriers into the systems that prevent their end-users from actions that – intentionally or not – could lead to serious cyber breaches and incidents. Cooperation and information sharing between CSIRTs was important in informing such strategies by providing insights about end-user behaviours leading to those cyber breaches and incidents. However, according to Bibi van den Berg and Esther Keymolen:

> While it is true that techno-regulation may prevent end users from making mistakes that can have a negative effect on their own cybersecurity or that of others, using this strategy will not weed out the biggest threat to security: that of intentional attackers. Hackers, cybercriminals, and those who engage in acts of cyber-espionage or cyber-terrorism go to great lengths to find weaknesses in systems and services and to exploit these to their benefit. Currently, the risks posed by these intentional attackers are considered to be far greater (both in terms of probability of occurrence and in terms of impact) than those created by genuine errors that random end users will make. Techno-regulatory interventions, or more generally the idea that a system's design will delineate the action space of end users, have no effect on those who intentionally seek to exploit vulnerabilities in it.[23]

A significant recent trend is that advanced attackers tend to select their targets carefully and do not aim to propagate malware by spreading it to many organisations across different sectors and countries with an expectation to infect a large number of (often indiscriminate) targets – a situation in which wide circulation of threat intelligence is usually helpful and effective in preventing further incidents. Instead, attackers keep hitting very few carefully chosen individual targets repeatedly while, at the same time, using highly sophisticated techniques to avoid attribution. Most importantly, they tend not to repeat what they have tried before.[24]

Trend towards customisation of cyber-attacks means that circulating information within the global CSIRT community has become less effective in reducing the damage

Such highly customised (tailor-made) attacks affect only some specific targets in a certain country at a particular point in time and thus are not replicated or repeated elsewhere (or even against the same target). Along with

[21] Japan International Cooperation Agency (JICA), " PacCERT オフィスの仮オープンと業務開始" [Temporary opening of PacCERT office and start of business], 12 July 2012, https://www.jica.go.jp/project/fiji/002/news/20120712.html.

[22] Paul Wilson, "CERTs and Cyber Security in the Pacific," APNIC, 9 May 2017, https://blog.apnic.net/2017/05/09/certs-cyber-security-pacific/; Standards Australia, "Pacific Islands Cyber Security Standards Cooperation Agenda," January 2020, https://www.standards.org.au/getattachment/engagement-events/international/Cyber-Security/Pacific-Islands-Cyber-Security-Standards-Cooperation-Agenda.pdf.aspx.

[23] Bibi van den Berg and Esther Keymolen, "Regulating Security on the Internet: Control versus Trust," *International Review of Law, Computers and Technology* 31 (2) (2017): 193, https://www.tandfonline.com/doi/full/10.1080/13600869.2017.1298504.

[24] For example, it is a common technique for a malware to connect to servers with different domain names. See: "Dynamic Resolution: Domain Generation Algorithms," MITRE ATT&CK, Mitre Corporation, last modified 2 October 2020, https://attack.mitre.org/techniques/T1568/002/.

attackers becoming harder to spot, this trend towards customisation of cyber-attacks means that circulating information within the global CSIRT community has become less effective in reducing the damage.

2.3. Commercialisation

As only some among many actors in cyberspace, CSIRTs are no longer the only expert groups on cybersecurity, as they used to be. In particular, commercial security product or service providers are playing a significant and more dominant role. In Japan alone, for example, the cybersecurity market was worth over $9 billion in 2018 and is expected to reach $10 billion by 2021.[25] As the market expands and security vendors attract talented technicians, it is no wonder that the quality and quantity of information gathered by CSIRTs has declined.

Security researchers are incentivised to sell their valuable findings, rather than sharing them openly

It is also important to highlight that security researchers are incentivised to sell their valuable findings, rather than sharing them openly. In the case of information on vulnerability in popular software (such as the Android OS and web browsers), this can be sold at a high price.[26] There are also bug bounty programmes operated by vendors and third parties. It is difficult to expect people to share their findings openly when alternatives that generate income are possible. Thus, it is reasonable to assume that the information shared with CSIRTs will fall in both quality and volume.

2.4. National CSIRTs becoming governmental organisations

The specific roles of national CSIRTs are particularly difficult to understand due to the lack of publicly available information. Looking back at previous studies, some have pointed out that the diversity of funding sources, mandates and organisational structures undermines their credibility.[27] The position of the national CSIRTs has become more complicated since those studies were conducted. As a major development influencing the efficiency of CSIRTs, almost all national CSIRTs in major countries have, over the last 30 years, grown to be mainly governmental in their function.

Only a few countries remain with national CSIRTs independent of government

For example, the UK, Canada, Australia and New Zealand placed a cybersecurity centre directly under the prime minister's office between 2016 and 2018. Only a few countries remain with national CSIRTs independent of government, such as Japan and Brazil. The proximity of intelligence agencies and militaries to national CSIRTs is another concern with this arrangement. Finally, national CSIRTs have begun to play additional roles such as public attribution of cyber-attacks, making international cooperation between CSIRTs even more difficult.

Conclusions

This chapter first described the development of CSIRTs and their community, which has since 1990 grown into a worldwide network. CSIRTs played an essential role in ensuring cybersecurity during the dawn of the Internet era. The UN GGE recognised their unique position in 2015, even describing them as

[25] Japan Network Security Association (JNSA) Market Research Working Group, "国内情報セキュリティ市場" [Domestic Information Security Market Survey], presentation, 23 April 2020, https://www.jnsa.org/result/surv_mrk/2020/2019_mktreport_new.pdf.

[26] Further consideration is needed to understand the price dynamics of different vulnerabilities. For example, Zerodium provides an interesting analysis, presenting a price list of vulnerabilities. See: "Our Exploit Acquisition Program," Zerodium, last accessed 26 March 2021, https://zerodium.com/program.html.

[27] Alexander Klimburg and Hugo Zylberberg, *Cyber Security Capacity Building: Developing Access* (Oslo: Norwegian Institute of International Affairs, 2015), https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/301986/NUPI_Report_6_15.pdf?sequence=3&isAllowed=y; Morgus et al, "National CSIRTs."

"a model of a decentralised, self-organised community".[28] However, as we have seen, international collaboration among CSIRTs is facing challenging times.

To summarise the issues relating to the development of and cooperation between CSIRTs, it can be said that this primarily stems from the zero-sum nature of cybersecurity and international relations. It is evident that the CSIRTs' culture of reciprocity is fluctuating. In this situation, the CSIRT community is required to redefine its purpose.

There is the possibility of the community developing into a cyber version of the International Red Cross, a network independent of governments, with the aim of maintaining stability in cyberspace from the perspective of humanitarian security

There are at least three choices. First, there is the possibility of the community developing into a cyber version of the International Red Cross, a network independent of governments, with the aim of maintaining stability in cyberspace from the perspective of humanitarian security.

In the public health approach to cyberspace, the CSIRT community can play a role as a source of scientific data for international cooperation in cyberspace

In this case, CSIRTs are expected to act based on the new values of system integrity and humanitarian protection, not on the interests of the particular country or organisation to which they belong.[29]

The second is the possibility of developing a cyber version of the World Health Organization (WHO) or of the US Centers for Disease Control and Prevention (CDC), with the common goal of "ensuring public health in cyberspace". In addition, as Jason Healey and Robert Knake argue, experts need to be able to communicate based on facts and correct measurement.[30] Throughout history, international networks of scientists have played a unique role in addressing this global challenge and, in the public health approach to cyberspace, the CSIRT community can play a role as a source of scientific data for international cooperation in cyberspace.

The third option is for CSIRTs to continue to become governmental bodies under each country's administration and concentrate on implementing that government's policies. But this could be viewed as a scenario to end the global CSIRT community able to collaborate mutually to achieve common goals. On a positive note, however, many have pointed to the lack of technical expertise in cyberspace policy discussions, and there are high hopes for CSIRTs as a means to fill this gap. Although not explicitly stated, the "no attack on CSIRTs" norm adopted by the UN GGE may refer to national CSIRTs. This can be interpreted as there may also be a role for CSIRTs in confidence building.

As a sub-scenario of the third option, cooperation may increasingly be advanced within certain "bubbles" with higher degrees of trust and alignment of interests. There are attempts to forge global techno-alliances of democracies that would collaborate closely in developing common standards and approaches. For instance, leaders of the so-called "Quad", or Quadrilateral Security Dialogue (the US, Japan, India and Australia) have recently agreed at a summit to cooperate on developing, regulating and securing emerging technologies.[31] Some Asian non-democracies are strengthening umbrella cooperation under, for instance, the Shanghai Cooperation Organisation.[32] These phenomena

[28] Tanczer, Brass, and Carr, "CSIRTs and Global Cybersecurity," 63.

[29] Duncan B. Hollis, "An E-SOS for Cyberspace," *Harvard International Law Journal* 52 (2) (2011), 373–432.

[30] Jason Healey and Robert K. Knake, *Zero Botnets: Building a Global Effort to Clean Up the Internet* (New York, NY: The Council on Foreign Relations, 2018), https://cdn.cfr.org/sites/default/files/report_pdf/CSR83_HealeyKnake_Botnets_0.pdf.

[31] Matthew P. Goodman and Dylan Gerstel, "Allied Technology Cooperation: Opportunities and Challenges," Center for Strategic and International Studies (CSIS), 23 March 2021, https://www.csis.org/analysis/allied-technology-cooperation-opportunities-and-challenges.

[32] Shanghai Cooperation Organization Secretariat, "Expansion of information technology cooperation in SCO discussed in Bishkek," 18 October 2019, http://eng.sectsco.org/news/20191018/590011.html.

may lead governmental CSIRTs of certain countries to cooperate more with each other than with those of other countries. They will be able to share highly sensitive information between the governments and the CSIRTs.

Estonia and Japan are expected to continue to provide stable and sustained support for developing and less developed countries

Estonia and Japan are expected to continue to provide stable and sustained support for developing and less developed countries, operating in accordance with the second option, i.e. the public health approach. According to Cybil's survey, 669 cyber capacity-building projects are currently ongoing globally.[33] And 594 different actors are engaging in this area. For example, Japan's JPCERT/CC has been active in Africa and other regions. In addition, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and other organisations have been providing support to member states of the Association of Southeast Asian Nations (ASEAN). Estonian expertise is also highly appreciated in the rest of the world. Estonia could, for instance, accelerate and build upon ongoing capacity-building projects such as Cyber4Dev.[34]

History tells us that, when there is a significant change in industry or technology, a private regime is formed to cope with it, and then it is transformed into an international or inter-state regime.[35] If this is the case, the future of CSIRTs is part of the larger question of who will dominate cyberspace. It is also an issue that cannot be separated from the effectiveness of nation-states in today's society.

The future of CSIRTs is part of the larger question of who will dominate cyberspace. It is also an issue that cannot be separated from the effectiveness of nation-states in today's society

[33] "The Knowledge Portal for Cyber Capacity Building," Cybil, last accessed 26 March 2021, https://cybilportal.org/.

[34] "Project objectives," Cyber 4D, last accessed 26 March 2021, https://cyber4dev.eu/project-activities/.

[35] Craig N. Murphy, "Global Governance: Poorly Done and Poorly Understood," *International Affairs* 76 (4) (2000): 789–803.

Overall Conclusions and Recommendations

The cyber domain has evolved dramatically over the last decade or so. Cyber power is no longer a theoretical concept and is integrated into the everyday statecraft of nations pursuing, projecting and protecting their interests and values internationally. This statecraft also interacts with, and must contend with, the interests and actions of multiple non-state actors. Fundamentally, the cyber domain has come to echo and channel geopolitical tensions and turbulence in the same way as other security domains – political, military, economic or societal. Cybersecurity is now firmly part of the complex, multilayered and dynamic management of the security environment that every responsible government undertakes in its efforts to counter threats to national security. In short, it is now a fully mature – if still dynamically evolving – field not just of multidisciplinary study but also of political and governance practice.

Fundamentally, the cyber domain has come to echo and channel geopolitical tensions and turbulence in the same way as other security domains – political, military, economic or societal

Estonia and Japan differ in many ways and inhabit apparently very different regional security complexes, but their perspectives towards and practices related to cybersecurity policy nevertheless align strongly. Much of Japan's cyber-threat landscape, highlighted by Jun Osawa in Chapter I, also applies to Estonia, as do the insights contained in this chapter concerning the need to develop cooperation strategies to achieve comprehensive cyber deterrence. Many of the challenges in developing Estonia's national cybersecurity strategy underlined by Kadri Kaska, Liis Rebane and Toomas Vaks in Chapter II – including the construction of an effective framework for building trust and cooperation between the government, public and private sectors – are equally pertinent to Japan. Despite differences in size and diplomatic reach, the two nations found solid common ground – as outlined by Anna-Maria Osula in Chapter III – in advancing international norms of responsible state behaviour in cyberspace. Last but not least, as pointed out by Koichiro Komiyama in Chapter IV, helping to build the cybersecurity capacity of other nations and providing incentives and policy frameworks for national CSIRTs to continue their cooperation is as relevant an undertaking for Estonia as it is for Japan.

There cannot be too much cooperation in cybersecurity between Estonia and Japan, and geopolitical and technological trends and developments will continue to provide much of its fuel

Cooperation – especially between like-minded democratic and open countries that share similar values and interests, such as Estonia and Japan – has been a key theme of this report. There cannot be too much cooperation in cybersecurity between these two nations, and geopolitical and technological trends and developments will continue to provide much of its fuel. It will serve as an antidote to growing collaboration between the assertive authoritarian powers and will offer opportunities for both countries to raise their profile, visibility and relevance in their respective parts of the world. Furthermore, the Indo-Pacific is an important new horizon for Estonia, given its growing pivotal role in the transatlantic and European policy agenda. Conversely, Northern Europe is emerging as an important gateway for Japan into the European and transatlantic arena.

Cybersecurity policy cooperation in bilateral and multilateral fora is one vehicle for both countries to advance their strategic objectives, both globally and regionally. As Estonia and Japan mark the centenary of diplomatic relations between them, this cooperation is taking centre stage. To consolidate, maintain and further expand it, we recommend focusing on the following directions and aspects related both to sharing national experience to enhance domestic capability development and to

cooperating on matters related to international security and the stability of cyberspace:

- With the aim of identifying and building policy-level collaboration frameworks between suitable counterparts among governmental organisations, the two countries should continue to develop initiatives to engage in dialogue and share national best practices on domestic cybersecurity governance (including openly sharing experiences on the development of national cybersecurity strategies, training programmes, etc.).

- Japan and Estonia would also benefit from exploring ways to develop further opportunities to exchange technical and operational data on cybersecurity, especially related to sharing acceptable levels of information on incident response and threat intelligence.

- Japan and Estonia will clearly continue to benefit from collaboration in bilateral or multilateral formats (e.g. via the EU-Japan framework or the UN) to promote common views on international cyber norms – from sharing legal assessments on the applicability of international law to the promotion of norms of responsible state behaviour and confidence-building measures.

- The two countries are also advised to engage in concerted diplomatic efforts to respond to and deter malicious state-sponsored cyber operations that endanger global cyber stability and go against agreed norms of responsible behaviour.

- As both nations recognise the responsibility to share experience stemming from their high level of development in cybersecurity, cooperating in international capacity-building initiatives to assist countries with lower levels of development is another important area for common efforts.

- Last but not least, the two countries should continue to support international research collaboration by bringing together researchers, academics and policy experts to share best practices and analysis related to common cybersecurity challenges.

List of References

Adamson, Liisi. "Let Them Roar: Small States as Cyber Norm Entrepreneurs." *European Foreign Affairs Review* 24, no. 2 (May 2019): 217–34. https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/24.2/EERR2019014.

Areng, Liina. *Lilliputian States in Digital Affairs and Cyber Security* (Tallinn Paper No. 4). Tallinn: NATO CCDCOE, 2014. https://ccdcoe.org/uploads/2018/10/TP_04.pdf.

Botek, Adam. "European Union establishes a sanction regime for cyber-attacks." *INCYDER*, NATO Cooperative Cyber Defence Centre of Excellence, 10 October 2019. https://ccdcoe.org/incyder-articles/european-union-establishes-a-sanction-regime-for-cyber-attacks/.

Bradshaw, Samantha. "Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity." Global Commission on Internet Governance Paper Series No. 23, Centre for International Governance Innovation and the Royal Institute of International Affairs (Chatham House), December 2015. https://www.cigionline.org/sites/default/files/gcig_no23web_0.pdf.

Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (Kindle Ed.). Oxford: Oxford University Press, 2017.

Center for Cyber and Homeland Security. *Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats.* Washington, DC: The George Washington University, 2016. https://wayback.archive-it.org/5184/20190103002934/https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

Chen, Joey, Hiroyuki Kakara, and Masaoki Shoji. *Operation ENDTRADE: TICK's Multi-Stage Backdoors for Attacking Industries and Stealing Classified Data.* TrendMicro Research, 2019. https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf.

Cheng, Dean. *Cyber Dragon: Inside China's Information Warfare and Cyber Operations.* Santa Barbara, CA: Praeger, 2016.

China Telecom. "Euro-Asia Network Solution." n.d.. https://www.chinatelecomeurope.com/wp-content/uploads/ChinaTelecom_Euro-Asia-network-solution.pdf.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* New York, NY: Harper Collins Publishers, 2010.

Council of the European Union. "Enhanced EU Security Cooperation in and with Asia: Council Conclusions." 9265/1/18 REV 1, 28 May 2018. https://www.consilium.europa.eu/media/35456/st09265-re01-en18.pdf.

Crandall, Matthew, and Collin Allan. "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms." *Contemporary Security Policy* 36, no. 2 (May 2015): 346–68. https://doi.org/10.1080/13523260.2015.1061765.

Cyber 4D. "Project objectives." Last accessed 26 March 2021. https://cyber4dev.eu/project-activities/.

Cyber Security Strategy Committee of Estonia. *Cyber Security Strategy.* Tallinn: Ministry of Defence, 2008. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy/@@download_version/993354831bfc4d689c20492459f8a086/file_en.

Cyber4DEV. "We are Cyber 4 Dev." Last accessed 18 February 2021. https://cyber4dev.eu/.

Cybil. "The Knowledge Portal for Cyber Capacity Building." Last accessed 26 March 2021. https://cybilportal.org/.

e-Governance Academy Foundation. "NCSI: Ranking." Accessed 7 February 2021. https://ncsi.ega.ee/ncsi-index/.

ENISA. "National Cyber Security Strategies – Interactive Map." Last accessed 26 March 2021. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

– . *ENISA Threat Landscape: The Year in Review.* Attika: European Union Agency for Cyber Security, 2020. https://www.enisa.europa.eu/publications/year-in-review/at_download/fullReport.

Estonian Information System Authority. *Annual Cyber Security Assessment 2017.* Tallinn: Estonian Information System Authority, 2017. https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria_csa_2017.pdf.

– . "ROCA Vulnerability and eID: Lessons Learned." n.d.. https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf.

EU CyberNet. "EU CyberNet – the bridge to cybersecurity expertise in the European Union." Last accessed 18 February 2021. https://www.eucybernet.eu/.

European Commission High Representative of the Union for Foreign Affairs and Security Policy. *The EU's Cybersecurity Strategy for the Digital Decade* (JOIN (2020)18 Final). Brussels: European Commission, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN.

European Commission. "Annex 3 of the Commission Implementing Decision on the 2019 Annual Action Programme for cooperation with third countries to be financed from the general budget of the European Union: Action Document for 'Security Cooperation in and with Asia'." 2019. https://ec.europa.eu/fpi/sites/fpi/files/annexe_3_security_cooperation_in_and_with_asia_part1_v2.pdf.

— . "Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade" (JOIN (2020)18 Final). EUR-Lex, Document 52020JC0018, 16 December 2020 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN.

Fackler, Martin. "Virus Infects Computers in Japan's Parliament." *The New York Times*, 25 October 2011. https://www.nytimes.com/2011/10/26/world/asia/virus-infects-computers-in-japans-parliament.html.

Federal Bureau of Investigations (FBI). "Update on Sony Investigation." Press release, 19 December 2014. https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

Feldstein, Steven. "The Global Expansion of AI Surveillance." Working Paper, Carnegie Endowment for International Peace, September 2019. https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.

Finnemore, Martha, and Duncan B. Hollis. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110, no. 3 (July 2016): 425–79. https://doi.org/10.1017/S0002930000016894.

Finnemore, Martha, and Kathryn Sikkink. "International Norm Dynamics and Political Change." *International Organization* 52, no. 4 (1998): 887–917.

FireEye. "APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat." FireEye Blog, 6 April 2017. https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html.

FIRST. "Computer Security Incident Response Team (CSIRT) Services Framework (Version 2.1)." November 2019. https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf.

— ."Product Security Incident Response Team (PSIRT) Services Framework (Version 1.1)." Spring 2020. https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1.pdf.

— . "Statement Regarding Huawei's Suspension from the Forum of Incident Response and Security Teams (FIRST)." 18 September 2019. https://www.first.org/newsroom/releases/20190918.

Freedom House. *Freedom on the Net 2020: The Pandemic's Digital Shadow.* Washington, DC: Freedom House, 2020. https://freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf.

GIP Digital Watch. "UN GGE and OEWG." Last accessed 26 March 2021. https://dig.watch/processes/ungge.

Goodman, Matthew P., and Dylan Gerstel. "Allied Technology Cooperation: Opportunities and Challenges." Center for Strategic and International Studies (CSIS), 23 March 2021. https://www.csis.org/analysis/allied-technology-cooperation-opportunities-and-challenges.

Government of Canada. *Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada.* Ottawa: Government of Canada, 2010. http://docshare01.docshare.tips/files/4043/40432912.pdf.

Government of Japan. *Cybersecurity Strategy 2018.* Tokyo: NISC, 2018. https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf.

Harrington, H. James, and Thomas McNellis. "Mobilizing the Right Lean Metrics for Success." *Quality Digest,* May 2006. https://www.qualitydigest.com/may06/articles/02_article.shtml.

Healey, Jason, and Robert K. Knake. *Zero Botnets: Building a Global Effort to Clean Up the Internet.* New York, NY: The Council on Foreign Relations, 2018. https://cdn.cfr.org/sites/default/files/report_pdf/CSR83_HealeyKnake_Botnets_0.pdf.

Hollis, Duncan B. "An E-SOS for Cyberspace." *Harvard International Law Journal* 52 (2) (2011): 373–432.

Huawei. "Huawei Marine and Tropical Science Commences Work on the Construction of the PEACE Submarine Cable Linking South Asia with East Africa." 6 November 2017. https://www.huawei.com/en/news/2017/11/PEACE-Submarine-Cable-SouthAsia-EastAfrica.

International Telecommunication Union (ITU). *Global Cybersecurity Index (GCI) 2017.* Geneva: ITU-D, 2017. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf.

— . *Global Cybersecurity Index (GCI) 2018.* Geneva: ITU-D, 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

International Telecommunication Union, World Bank, Commonwealth Secretariat, Commonwealth Telecommunications Organisation, and NATO Cooperative Cyber Defence Centre of Excellence. *Guide to Developing a National Cybersecurity Strategy – Strategic Engagement in Cybersecurity.* Geneva: The International Telecommunication Union, 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

IPA. *標的型攻撃メールの分析に関するレポート* [Report on the analysis of targeted attack emails]. IPA, 2011. https://www.ipa.go.jp/files/000009375.pdf.

Iran Action Group and Iran Office of the Bureau for Near Eastern Affairs. *Outlaw Regime: A Chronicle of Iran's Destructive Activities* (2020 Edition). Washington, DC: US Department of State, 2020. https://www.state.gov/wp-content/uploads/2020/09/Outlaw-Regime-2020-A-Chronicle-of-Irans-Destabilizing-Activity.pdf.

"Japan defence firm Mitsubishi Heavy in cyber attack." *BBC News*, 20 September 2011. https://www.bbc.com/news/world-asia-pacific-14982906.

Japan International Cooperation Agency (JICA). "PacCERTオフィスの仮オープンと業務開始" [Temporary opening of PacCERT office and start of business]. 12 July 2012. https://www.jica.go.jp/project/fiji/002/news/20120712.html.

Japan Network Security Association (JNSA) Market Research Working Group. "国内情報セキュリティ市場" [Domestic Information Security Market Survey]. Presentation, 23 April 2020. https://www.jnsa.org/result/surv_mrk/2020/2019_mktreport_new.pdf.

Jasper, Scott. *Strategic Cyber Deterrence.* Lanham, MD: Rowman & Littlefield, 2017.

Jun, Jenny, Scott LaFoy, and Ethan Sohn. *North Korea's Cyber Operation: Strategy and Response* (CSIS Korea Chair Report). Washington, DC: Center for Strategic and International Studies, 2015. http://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf.

Keck, Zachary. "South Korea Hit by Cyber Attack – North Korea to Blame?." *The Diplomat*, 21 March 2013. https://thediplomat.com/2013/03/south-korea-hit-by-cyber-attack-north-korea-to-blame/.

Keyes, Daniel, and Greg Magana. "REPORT: Chinese fintechs like Ant Financial's Alipay and Tencent's WeChat are rapidly growing their financial services ecosystems." *Business Insider*, 19 December 2019. https://www.businessinsider.com/china-fintech-alipay-wechat.

Klimburg, Alexander, and Hugo Zylberberg. *Cyber Security Capacity Building: Developing Access.* Oslo: Norwegian Institute of International Affairs, 2015. https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/301986/NUPI_Report_6_15.pdf?sequence=3&isAllowed=y.

Klimburg, Alexander, ed. *National Cyber Security Framework Manual.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012. https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf.

Lachow, Irving. "Active Cyber Defense: A Framework for Policymakers." CNAS Policy Brief, Center for a New American Security, February 2013. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS_ActiveCyberDefense_Lachow_0.pdf?mtime=20160906080446&focal=none.

Lee, Robert M. "The Sliding Scale of Cyber Security." SANS Analyst White Paper, SANS Institute, August 2015. https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240.

Lewis, James. "Overview of the Cyber Stability Framework: Norms of Responsible State Behaviour, International Law, Confidence and Capacity Building Measures." Tallinn Winter School of Cyber Diplomacy, 9–10 February 2021, https://vm.ee/et/node/53915.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain.* Oxford: Oxford University Press, 2015.

Macnica Networks. *標的型攻撃の実態と対策アプローチ* [The reality of targeted attacks: Counter-measures approach]. Macnica Networks Corporation, 2016. https://www.macnica.net/file/security_report_20160613.pdf.

Maidment, Gary. "SAIL the Atlantic with CAMTEL." *WinWin*, 21 April 2018. https://www.huawei.com/en/publications/winwin-magazine/31/sail-the-atlantic-with-camtel.

Mälksoo, Lauri, and Adam Lupel. "A Necessary Voice: Small States, International Law, and the UN Security Council." Blog, ETH Zürich Center for Security Studies, 29 April 2019. https://css.ethz.ch/en/services/digital-library/articles/article.html.

Mankoff, Jeffrey. "Russian Influence Operations in Germany and Their Effect." CSIS Commentary, Center for Strategic and International Studies (CSIS), 3 February 2020. https://www.csis.org/analysis/russian-influence-operations-germany-and-their-effect.

Ministère des Armées (Ministry of Armed Forces). *Droit International Appliqué Aux Opérations Dans Le Cyberspace* [International Law Applied to Cyberspace Operations]. Paris: Délégation à l'information et à la communication de la défense, 2019. https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf.

Ministry of Defence of Japan. "防衛関連企業に対する不正アクセス事案について" [Unauthorised access to defence companies]. Press release, 6 February 2020, https://www.mod.go.jp/j/press/news/2020/02/06c.pdf.

Ministry of Economic Affairs and Communications of Estonia. *Cyber Security Strategy 2014-2017.* Tallinn: Ministry of Economic Affairs and Communications, 2014. https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.

— . *Cybersecurity Strategy 2019-2022: Republic of Estonia.* Tallinn: Ministry of Economic Affairs and Communications, 2019. https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

Ministry of Foreign Affairs and Trade of New Zealand. "The Application of International Law to State Activity in Cyberspace." 1 December 2020. https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf.

Ministry of Foreign Affairs of Japan. "Speech by Prime Minister Abe at the World Economic Forum Annual Meeting." 23 January 2019, https://www.mofa.go.jp/ecm/ec/page4e_000973.html.

Ministry of Foreign Affairs of the People's Republic of China. "Full text of President Xi's speech at opening of Belt and Road forum." 15 May 2017. https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1465819.shtml.

Minji, Lee. "Gov't confirms Pyongyang link in March cyber attacks." *Yonhap News*, 10 April 2013. https://en.yna.co.kr/view/AEN20130410007352320.

Mitre Corporation. "Dynamic Resolution: Domain Generation Algorithms." MITRE ATT&CK. Last modified 2 October 2020. https://attack.mitre.org/techniques/T1568/002/.

Mitsubishi Electric Corporation. "不正アクセスによる個人情報と企業機密の流出可能性について" [About the possibility of leakage of personal information and trade secrets due to unauthorised access]. Press release, 20 January 2020, https://www.mitsubishielectric.co.jp/news/2020/0120-b.pdf.

Morgus, Robert, Isabel Skierka, Mirko Hohmann, and Tim Maurer. *National CSIRTs and Their Role in Computer Security Incident Response*. Washington, DC: New America and Global Public Policy Institute, 2015. https://static.newamerica.org/attachments/11916-national-csirts-and-their-role-in-computer-security-incident-response/CSIRTs-incident-response_2-2016.eea78f5a4748443d8000903e300d5809.pdf.

Murphy, Craig N. "Global Governance: Poorly Done and Poorly Understood." *International Affairs* 76 (4) (2000): 789–803.

Nagasako, Tomoko. "Global disinformation campaigns and legal challenges." *International Cybersecurity Law Review,* 1 (2020): 125-36.

Nai Fovino, Igor, G. Barry, S. Chaudron, I. Coisel, M. Dewar, H. Junklewitz, G. Kambourakis, I. Kounelis, B. Mortara, J. P. Nordvik, and I. Sanchez, eds. *Cybersecurity, Our Digital Anchor.* Luxembourg: Publications Office of the European Union, 2020. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC121051/cybersecurity_online.pdf.

National Center of Incident Readiness and Strategy for Cybersecurity (NISC). "日本年金機構における個人情報流出事案に関する 原因究明調査結果" [Results of the investigation into the cause of the leak of personal information at the Japan Pension Service]. 20 August 2015. https://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf.

NEC Corporation. "当社の社内サーバへの不正アクセスについて" [Unauthorised access to our internal server]. Press release, 31 January 2020. https://jpn.nec.com/press/202001/20200131_01.html.

Nye, Joseph S. "Deterrence and Dissuasion in Cyberspace." *International Security*, Vol. 41, No. 3 (Winter 2016/17): 44–71.

– . "The Regime Complex for Managing Global Cyber Activities." *Center for International Governance and Innovation (CIGI) Publications* (1) (2014): 1–15.

Office of the Director of National Intelligence. "Assessing Russian Activities and Intentions in Recent US Elections." 6 January 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Office of the President of Estonia. "Speech of the President of the Republic of Estonia at the Opening of CyCon 2019." 29 May 2019. https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html.

One Belt, One Road Construction Business Promotion Guidance Group Benkou Office. *「一帯一路」共同建設のイニシアチブ 進展、貢献と展望 2019* [The "One Belt, One Road" Joint Construction Initiative: Progress, Contributions and Prospects 2019]. Beijing: China International Book Trading Co, 2019. https://www.yidaiyilu.gov.cn/wcm.files/upload/CMSydylgw/201904/201904240813002.pdf.

Organisation for Security and Co-operation in Europe (OSCE). "Decision No. 1202. OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies." *PC Journal*, No. 1092 (March 2016). https://www.osce.org/files/f/documents/d/a/227281.pdf.

Osawa, Jun. "The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?." *Asia-Pacific Review,* vol. 24, No. 2 (2017): 113-31.

Owens, William A., Kenneth W. Dam, and Herbert S. Lin, eds. *Technology, Policy, Law, and Ethics. Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington, DC: The National Academies Press, 2009. https://doi.org/10.17226/12651.

PacCERT Working Group. "Pacific CERT (PacCERT)." Presentation, n.d. https://www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/docs/Pacific%20CERT%20(PacCERT).pptx.

Painter, Chris. "Deterrence in cyberspace. Spare the costs, spoil the bad state actor: Deterrence in cyber space requires consequences." ASPI Policy Brief / Report No.4, The Australian Strategic Policy Institute, 2018. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2018-05/Deterrence%20in%20cyberspace_0.pdf?JtY9WhXLd53pCnni2U5PiHr8ikcPMC5I.

Permanent Mission of Estonia to the UN. "At Estonia's Initiative, the International Community Reaffirmed the Importance of Cyber Stability, Including during the COVID-19 Crisis, at the UN Security Council." 23 May 2020. https://un.mfa.ee/at-estonias-initiative-the-international-community-reaffirmed-the-importance-of-cyber-stability-including-during-the-covid-19-crisis-at-the-un-security-council/.

— . "Opening Statement by the Republic of Estonia, By Amb. Heli Tiirmaa-Klaar for the UN GGE Panel on Regional Consultations." 2019. https://www.un.org/disarmament/wp-content/uploads/2019/12/estonia-gge-panel-on-regional-consultations-05-12-2019.pdf.

— . "Stakeout on Cyber-Attack against Georgia by Estonia, the United Kingdom and the United States." 5 March 2020. https://un.mfa.ee/press-stakeout-by-estonia-the-united-kingdom-and-the-united-states-on-cyber-attack-against-georgia/.

Pernik, Piret. *Küberjulgeoleku strateegia 2008–2013 analüüs* [Analysis of the cybersecurity strategy 2008–13]. Tallinn: Rahvusvaheline Kaitseuuringute Keskus, 2013.

Raymond, Mark. "Managing Decentralised Cyber Governance: The Responsibility to Troubleshoot." *Strategic Studies Quarterly* 10 (4) (2016): 123–49.

Reuters. "North Korean hackers said possibly behind massive Coincheck heist." *The Japan Times*, 6 February 2018. https://www.japantimes.co.jp/news/2018/02/06/business/tech/north-korean-hackers-said-possibly-behind-massive-coincheck-heist/.

Riigikogu. "Administrative Procedure Act." *Riigi Teataja* (State Gazette), RT I 2001, 58, 354 (27 March 2019) (translation). https://www.riigiteataja.ee/en/eli/527032019002/consolide.

Sanger, David E., Michael S. Schmidt, and Nicole Perlroth. "Obama Vows a Response to Cyberattack on Sony." *The New York Times,* 19 December 2014. https://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html.

Sanger, David. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power.* New York, NY: Crown Publisher, 2012.

Schmitt, Michael. "Estonia Speaks Out on Key Rules for Cyberspace." Just Security, 10 June 2019. https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/.

Secretariat of the Pacific Community. "Pacific Regional ICT Ministers' Meeting 2010: Information and communication technology for development, governance and sustainable livelihoods of Pacific communities." *e-talanoa,* Issue 1 (2010): 2. https://www.jica.go.jp/project/fiji/002/materials/pdf/e_talanoa_issue_01_01.pdf;

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age.* New York, NY: Public Affairs, 2016.

Shanghai Cooperation Organization Secretariat. "Expansion of information technology cooperation in SCO discussed in Bishkek." 18 October 2019. http://eng.sectsco.org/news/20191018/590011.html.

Skierka, Isabel, Robert Morgus, Mirko Hohmann, and Tim Maurer. "CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams." Working Paper, Global Public Policy Institute & New America, May 2015. https://static.newamerica.org/attachments/2943-csirt-basics-for-policy-makers/CSIRT%20Basics%20for%20Policy-Makers%20May%202015%20WEB%2009-15.16efa7bcc9e54fe299ba3447a5b7d41e.pdf.

Spykman, Nicolas J. *The Geography of the Peace.* New York, NY: Harcourt, Brace & Co., 1944.

Stadnik, Ilona. "Discussing State Behaviour in Cyberspace: What Should We Expect?." DiploFoundation, 20 March 2019. https://www.diplomacy.edu/blog/discussing-state-behaviour-cyberspace-what-should-we-expect.

Standards Australia. "Pacific Islands Cyber Security Standards Cooperation Agenda." January 2020. https://www.standards.org.au/getattachment/engagement-events/international/Cyber-Security/Pacific-Islands-Cyber-Security-Standards-Cooperation-Agenda.pdf.aspx.

Tanczer, Leonie Maria, Irina Brass, and Madeline Carr. "CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy." *Global Policy* 9 (November 2018): 60–6.

The White House. *National Cyber Strategy of the United States of America.* Washington, DC: The White House, 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Tikk, Eneken, Kadri Kaska, and Liis Vihul. *International Cyber Incidents: Legal Considerations.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010. https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf.

"Transcript: President Xi Addresses the 2018 Boao Forum for Asia in Hainan." US-China Perception Monitor, 18 April 2018. https://uscnpm.org/2018/04/11/transcript-president-xi-addresses-2018-boao-forum-asia-hainan/.

Trend Micro, "The Hack of Sony Pictures: What We Know and What You Need to Know." 8 December 2014. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know.

US Chamber of Commerce. *Made in China 2025: Global Ambitions Built on Local Protections.* Washington, DC: US Chamber of Commerce, 2017. https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf.

US Department of Commerce Bureau of Industry and Security. "Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List, effective August 19, 2019 (84 FR 43493)." Federal Register Notices 2019, 21 August 2019. https://www.bis.doc.gov/index.php/federal-register-notices/17-regulations/1541-federal-register-notices-2019#fr54002.

US Department of Defense. *The DoD Cyber Strategy.* Washington, DC: Department of Defense, 2015. https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.

US Department of Homeland Security and Federal Bureau of Investigations. "Grizzly Steppe – Russian Malicious Cyber Activity." 29 December 2016. https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

US Department of Justice Office of Public Affairs. "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace." Press release, 19 October 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

– ."Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe." Press release, 17 February 2021. https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

– ."U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." News release, 19 May 2014. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

US Department of State Office of the Coordinator for Cyber Issues. "Joint Statement on Advancing Responsible State Behavior in Cyberspace." 23 September 2019. https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

US Senate Committee on Commerce, Science and Transportation. "Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown." Hearings, 11 July 2018. https://www.commerce.senate.gov/2018/7/complex-cybersecurity-vulnerabilities-lessons-learned-from-spectre-and-meltdown.

UK Foreign, Commonwealth and Development Office. "UK exposes series of Russian cyber attacks against Olympic and Paralympic Games." Press release, GOV.uk, 19 October 2020. https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games.

United Nations Department of Economic and Social Affairs. *United Nations E-Government Survey: Digital Government in the Decade of Action for Sustainable Development.* New York, NY: United Nations, 2020. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf.

United Nations General Assembly. "Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the First Committee (A/73/505)." Seventy-third session, Agenda item 96, 19 November 2018. https://undocs.org/A/73/505.

United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *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, NY: United Nations, 2015, https://undocs.org/pdf?symbol=en/A/70/174.

United Nations Office for Disarmament Affairs. "2016 Submissions from Member States: Japan." 2016. https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/10/Japan.pdf.

– . "2017 Submissions from Member States: Estonia – Response to the General Assembly Resolution 70/237 on 'Developments in the Field of Information and Telecommunications in the Context of International Security'." 2017. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2017/09/Estonia-full.pdf;

– . "2017 Submissions from Member States: Japan." 2017. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2017/09/Japan.pdf.

– ."2019 Submissions from Member States: National Reply from Japan." 2019. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/Japan-2019.pdf.

– . "Briefing at the Security Council Virtual Arria-Formula Meeting on 'Cyber Stability, Conflict Prevention and Capacity Building': Remarks by Ms. Izumi Nakamitsu, High Representative for Disarmament Affairs." 22 May 2020. https://front.un-arm.org/wp-content/uploads/2020/05/UNSC-Arria-Formula-Meeting-on-Cybersecurity-HR-Remarks-22-May-2020.pdf.

– . "The Future of Discussions on ICTs and Cyberspace at the UN (Submission by France, Egypt, Argentina, Colombia, Ecuador, Gabon, Georgia, Japan, Morocco, Norway, Salvador, Singapore, the Republic of Korea, the Republic of Moldova, The Republic of North Macedonia, the United Kingdom, the EU and its member States – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, France, Finland, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden)." 8 October 2020. https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf.

United Nations Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. *Final Substantive Report* (A/AC.290/2021/CRP.2). New York, NY: United Nations, 2021. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

United Nations Security Council Panel of Experts. *Midterm report of the Panel of Experts Submitted Pursuant to Resolution 2464 (2019).* New York, NY: United Nations, 2019. https://undocs.org/S/2020/151.

— . *Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009).* New York, NY: United Nations, 2010. https://www.undocs.org/S/2010/571.

Vaks, Toomas. *Küberjulgeoleku strateegia mõju küberturvalisuse arengule Eestis 2008-2018* [The impact of cybersecurity strategy on the development of cybersecurity in Estonia in 2008–18]. Tallinn: Tallinna Tehnikaülikool, 2018. https://digikogu.taltech.ee/en/Download/fb794e52-07fd-4b49-93cb-3be2c56d95c2.

Van den Berg, Bibi, and Esther Keymolen. "Regulating Security on the Internet: Control versus Trust." *International Review of Law, Computers and Technology* 31 (2) (2017): 188–205. https://www.tandfonline.com/doi/full/10.1080/13600869.2017.1298504.

West-Brown, Moira J., Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2nd Edition). Pittsburgh, PA: Carnegie Mellon Software Engineering Institute, 2003. https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf.

Wilson, Paul. "CERTs and Cyber Security in the Pacific." APNIC, 9 May 2017. https://blog.apnic.net/2017/05/09/certs-cyber-security-pacific/.

Winstead, Nicholas. "Hack-Back: Toward a Legal Framework for Cyber Self-Defense." Center for Security, Innovation, and New Technology, American University, 26 June 2020. https://www.american.edu/sis/centers/security-technology/hack-back-toward-a-legal-framework-for-cyber-self-defense.cfm.

Zerodium. "Our Exploit Acquisition Program." Last accessed 26 March 2021. https://zerodium.com/program.html.

Zetter, Kim. *Countdown to ZeroDay: Stuxnet and the Launch of the World's First Digital Weapon.* New York, NY: Crown Publishers, 2014.

RECENT ICDS PUBLICATIONS

REPORTS

Hurt, Martin, and Tiia Sõmer. ***Cyber Conscription: Experience and Best Practice from Selected Countries***. Tallinn: International Centre for Defence and Security, February 2021.

Juurvee, Ivo, and Mariita Mattiisen. ***The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict.*** Tallinn: International Centre for Defence and Security, August 2020.

Sherr, James. ***Nothing New Under the Sun? Continuity and Change in Russian Policy Towards Ukraine.*** Tallinn: ICDS Estonian Foreign Policy Institute, July 2020.

Jermalavičius, Tomas, Priit Mändmaa, Emma Hakala, Tomas Janeliūnas, Juris Ozoliņš, and Krystian Kowalewski. ***Winds of Change, or More of the Same? Impact of the 2018-19 Election Cycle on Energy Security and Climate Policies in the Baltic states, Poland and Finland.*** Tallinn: International Centre for Defence and Security, May 2020.

BOOKS

Raik, Kristi, and András Rácz (eds.). ***Post-Crimea Shift in EU-Russia Relations: From Fostering Interdependence to Managing Vulnerabilities.*** Tallinn: ICDS Estonian Foreign Policy Institute, 2019.

POLICY PAPERS

Helwig, Niklas, Juha Jokela, Piret Kuusik, and Kristi Raik. "**A Northern Agenda for an Open and Secure Europe: Nordic-Baltic Perspectives on European Sovereignty and Strategic Autonomy.**" ICDS/EFPI Policy Paper, May 2021.

Stoicescu, Kalev. "**NATO's Southern Neighbourhood: The Alliance Needs a Strategy for the Regions to its South.**" ICDS Policy Paper, February 2021.

Loik, Ramon. "**Volunteers in Estonia's Security Sector: Opportunities for Enhancing Societal Resilience.**" ICDS Policy Paper, June 2020.

Baranowski, Michał, Linas Kojala, Toms Rostoks, and Kalev Stoicescu. Tony Lawrence (editor). "**What Next for NATO? Views from the North-East Flank on Alliance Adaptation**." ICDS Policy Paper, June 2020.

ANALYSES

Janeliūnas, Tomas. "**The Long Shadow of a Nuclear Monster: Lithuanian responses to the Astravyets NPP in Belarus.**" ICDS Analysis, March 2021.

Allik, Sten, Sean F. Fahey, Tomas Jermalavičius, Roger McDermott, and Konrad Muzyka. "**The Rise of Russia's Military Robots: Theory, Practice and Implications.**" ICDS Analysis, February 2021.

Vseviov, Jonatan. "**Constructing Deterrence in the Baltic States.**" ICDS Analysis, February 2021.

Kuusik, Piret. "**Under Pressure: Nordic-Baltic Cooperation During the COVID-19 Crisis.**" ICDS/EFPI Analysis, February 2021.

Teperik, Dmitri, and Oksana Iliuk. "**The Universe of Resilience: From Physics of Materials Through Psychology to National Security.**" ICDS Analysis, January 2021.

All ICDS publications are available from https://icds.ee/category/publications/.


ICDS.Tallinn


@ICDS _ Tallinn


ICDS-Tallinn


www.icds.ee

ISSN 2228-0529
ISBN 978-9916-9657-0-2 (PRINT)
ISBN 978-9916-9657-1-9 (PDF)

International Centre for Defence and Security
63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee