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.

> *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"*

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

[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.