Strengthening Public-Private Partnership in Cyber Defense: A Comparison with the Republic of Estonia*

YAMAGUCHI Yoshihiro[1]**

Abstract

This paper looks at Japan's cybersecurity policies while placing the focus on the defense of critical infrastructure that is directly related to national security, and examines the measures that need to be put in place going forward in regard to public-private partnership initiatives. Firstly, it takes a broad overview of Japan's policies followed by an overview of the cybersecurity policies of the Republic of Estonia, and carries out a comparison with Japan based on the following six classifications: cybersecurity strategy, legal systems, public-private partnership organizations and information-sharing systems, risk analysis and business continuity plans, cyber exercises, and national defense strategy and organizations. Then, the feasibility of implementation in Japan is considered. Finally, it makes the following recommendations: (1) Positioning the protection of critical infrastructure as the most important issue in the cybersecurity strategy; (2) Reviewing the legal system and strengthening the supervision and guidance of critical information infrastructure (CII) operators; (3) Strengthening the authority of the National center of Incident readiness and Strategy for Cybersecurity (NISC), and enhancing its functions; (4) Implementing exercises in preparation for a large-scale cyberattack at the national level; (5) Building a framework that enables civilians with advanced skills to participate in national defense in cyberspace.

Introduction

Late at night on April 27, 2007, a cyberattack was launched on the websites of the Estonian government and media organizations in the private sector. Initially, this had been a Denial of Service (DoS) attack that employed the simple method of sending ping commands in a concentrated attack to the target server. However, the methods used became increasingly sophisticated. The domain name system (DNS) of Estonia's leading Internet service provider (ISP) became targets of the attacks, and Distributed Denial of Service (DDoS) attacks were carried out simultaneously from

* Originally published in Japanese in *Boei Kenkyusho Kiyo* [NIDS Security Studies], vol.21, no.1, December 2018. Some parts have been updated.

** Information and Communications Section, Defense and Operations Division, Air Staff Office

1 This paper contains additions and revisions made to a paper submitted for the 65th General Course (Graduate School Partnership Program) of the National Institute for Defense Studies (NIDS). The views expressed in this paper are those of the author and do not represent the views of the author's organization. The author would like to thank Prof. Yasuaki Hashimoto, Director, Policy Studies Department, NIDS, Prof. Atsushi Sunami, Executive Advisor to the President, National Graduate Institute for Policy Studies (GRIPS), and Prof. Narushige Michishita, GRIPS, for their guidance in preparing this paper and NIDS for providing research space.

multiple botnets. As a result, Internet communications were interrupted intermittently.

From midnight of May 9 (Moscow time), which is also Russia's Victory Day, to May 10, the DDoS attacks reached their peak, and the operation of 58 websites including those of government agencies was simultaneously interrupted, forcing many banks to suspend their business operations. By May 18 when the attacks subsided, the Congress, government ministries and agencies, ISP, telephone networks, mass media, banks, and credit card companies were among the organizations that had been targeted. The attacks included DDoS attacks, tampering with webpages, attacks on DNS servers, and the jamming of communications through mass spam mails.[2]

During the cyberattack that lasted approximately three weeks, the Computer Emergency Response Team-Estonia (CERT-EE) provided 24-hour response and support for the large-scale cyberattack, while receiving assistance from volunteer cybersecurity experts from Estonia and abroad. With regard to the DDoS attacks, CERT-EE worked in cooperation with communications carriers and security companies to expand bandwidth for governmental networks and reinforce server processing capability, as well as install firewalls. At the same time, through analyses on the patterns of the attack, it successfully interrupted many attacks by establishing effective filtering rules for the ISPs.[3]

This large-scale cyberattack had been triggered by the Estonian government's decision to remove all monuments erected during the Soviet occupation. An old bronze statue of a Soviet soldier installed in the capital city of Tallinn had been erected to commemorate the victory of the Soviet army against Nazi Germany during the Second World War. For Estonians who were ethnic Russians, this statue was a symbol of a victory won by their motherland, Russia.

Figure 1 Bronze statue of a Soviet soldier and monument, prior to its relocation[4]

Source: Extracted from BBC news report (April 27, 2017)

However, this bronze statue was gradually transformed into a site of nationalism conflict as the result of a violent incident by Russian Estonians against non-Russian Estonians that took place near the bronze statue on May 9, 2006, Russia's Victory Day. The Estonian government, with a sense of crisis, announced in March 2007 that the bronze statue would be relocated to a cemetery for the war dead in the suburbs of Tallinn. On April 26, 2007, after the government erected a fence in the area in preparation for the relocation of the statue, Russian Estonians gathered in opposition

2 Tikk, E., Kaska, K., Vihul, L., *International Cyber Incidents: Legal Consideration* (NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), 2010), pp. 18-22.

3 Ibid., p. 24.

4 Damien McGuinness, How a cyber attack transformed Estonia, BBC News 27 April 2017, http://www.bbc.com/news/39655415.

of the move. This erupted into a riot that included acts of vandalism on the surrounding facilities. This riot resulted in one death, several hundred injured persons, and the arrest of about 1,300 people. Furthermore, an opposition demonstration unfolded in front of the Estonian embassy in Moscow, and even led to the assault of the Ambassador of Estonia to Russia.[5]

The large-scale cyberattack on Estonia occurred under these circumstances, and became known as the first attack in history carried out against a nation in cyberspace.[6]

Cyberspace has long been described as the "fifth domain of war" after land, sea, air, and space. Cyberattacks have developed to become one of the means of achieving the goals in political and diplomatic disputes between countries, as demonstrated by the examples of attacks in Estonia and Georgia, as well as the Stuxnet virus attack on Iran. Countries around the world view large-scale cyberattacks as an important national security issue; alongside with advancing cybersecurity policies at the national level, they have also established dedicated cyberwar units in their armies, such as the newly set up United States Cyber Command and the People's Liberation Army Strategic Support Force of China, and are moving forward on preparations for the cyberwars that are expected to happen in the near future. Japan, too, is steadily advancing cybersecurity measures at the national level. Within the Ministry of Defense and Self-Defense Forces, it has established a new Cyber Defense Group and is working to strengthen its coping mechanism.

In Japan, although there are incidents of information leakage, theft of corporate information, and hacking for financial profit, large-scale cyberattacks that cause serious damage to critical infrastructure have never occurred to date. Japan has problems such as territorial issues with neighboring countries and its perception of history, which can potentially trigger political and diplomatic disputes. It has also adopted a hardline stance with regard to North Korea's nuclear missile development issue, and is continuing to apply pressure primarily through economic sanctions. The Rugby World Cup and Tokyo Olympic and Paralympic Games will be held in Japan in 2019 and 2020 respectively. In view of these factors, it is likely that large-scale cyberattacks with political or diplomatic motives and cyberattacks that are used as a means of terrorism may be carried out on Japan's critical infrastructure. The means of carrying out cyberattacks are growing increasingly sophisticated year after year. In the event that a large-scale cyberattack is carried out using methods that are more complex and sophisticated than that of the Estonian incident that occurred about 10 years ago, will Japan be able to put in place effective response measures?

The purpose of this paper is to establish how public-private partnership initiatives have progressed with regard to the cybersecurity policies that Japan has been implementing to date, which are the measures that are superior to those of other countries, which are the areas that are lagging behind in its countermeasures, and what measures need to be put in place going forward. Among the extensive and wide-ranging cybersecurity policies, the analysis in this paper places the focus on the protection of critical infrastructure that is directly linked to national security.

The discussion in this paper is set out as follows. Firstly, section 1 establishes the importance of joint efforts by the public and private sectors to build a cyber defense system from the perspective of deterrence and the characteristics of cyberspace, and taking into account the current situation surrounding cyberattacks.

---

5 Tikk, *International Cyber Incidents: Legal Consideration*, p. 16.

6 Hiroshi Itoh, *"Daigo no Senjo: Saibasen no Kyoi"* [The Fifth Domain of War: The Threat of Cyberwar)], (Shodensha Shinsho, 2012), p. 142.

Next, section 2 verifies the current situation with regard to public-private partnership initiatives in the area of cyber defense in Japan, while Section 3 provides an overview of the various policies that the Republic of Estonia (hereafter, "Estonia") is implementing in its active efforts to advance public-private partnership on cyber defense for critical services, followed by a comparison with Japan and a review of the feasibility of implementing such policies in Japan. In comparing the respective policies of Estonia and Japan, this paper places particular focus on public-private partnership in the protection of critical infrastructure, and carries out its analysis based on the following six classifications: cybersecurity strategy, legal systems, public-private partnership organizations and information sharing systems, risk analysis and business continuity plans, cyber exercises, and national defense strategy and organizations.

Finally, in section 4, this paper offers recommendations of several policies aimed at promoting public-private partnership in cyber defense in Japan.

1. The Importance of Public-Private Partnership in Cyber Defense

Why is public-private partnership necessary in order to realize the defense of cyberspace? The answer to this question can be summarized in the following two points: (1) Cyberspace itself and much of the country's critical infrastructure is operated by the private sector; and, (2) To secure deterrent power in cyberspace, it is vital for the government to gain the cooperation of private-sector operators.

(1) Characteristics of cyberspace

Cyberspace, unlike the domains of land, sea, air, and space, is unique in the sense that it is a man-made domain. Cyberspace is composed of terminal equipment such as computers, smartphones, and network cameras, networks such as Local Area Network (LAN) cables, optical lines, Wi-Fi (wireless LAN), mobile phone networks, international submarine cables, and satellite communication lines, various software and applications that are installed in the terminals, and communications protocols such as TCP/IP (Transmission Control Protocol/Internet Protocol), HTTP (Hypertext Transfer Protocol), and SMTP (Simple Mail Transfer Protocol). All of these components are primarily maintained and operated by private-sector operators. Furthermore, with the rapid advancement of information and communications technology, all the systems that make up society have become networked, and Internet technology is now actively applied to the critical infrastructure of a country such as electricity, communications, water, gas, transportation, railroads, and finance, with the purposes of improving the efficiency of maintenance and management as well as saving manpower. A large-scale cyberattack on such critical infrastructure could paralyze the functions of a country and have a serious impact on citizens' lives and economic and social activities. Regardless of that, the majority of a country's critical infrastructure is maintained and operated by operators in the private sector.

As seen in the cases of Estonia, Syria, Georgia, and Ukraine, cyberattacks that are linked to military operations are being carried out in reality. In international armed conflicts, there is a strong likelihood for cyberattacks to be carried out not only on the central leadership of a country and its military organizations, but also on its critical infrastructure, in tandem with military operations conducted through conventional military forces or as a part of a surprise attack. Taking into consideration such characteristics of cyberspace and the dependence of critical infrastructure on the private sector, unlike the domains of land, sea, air, and space, it is difficult for the cyber defense unit

of a country's military force to defend the country alone. Rather, it is important to cooperate with many private-sector actors such as communications carriers, ISPs, manufacturers of information and communications equipment and software companies, security enterprises, and CII operators.

(2) Deterrence in cyberspace

Next, I would like to consider public-private partnership from the perspective of deterrence. The concept of deterrence is often categorized generally into deterrence by punishment and deterrence by denial. Deterrence by punishment involves applying pressure on the enemy's cost calculations based on the threat of delivering an unbearable blow, in order to make the enemy give up the idea of launching an attack. Deterrence by denial involves applying pressure on the enemy's calculations of the possibility of achieving its goal, based on the ability to physically deter specific offensive action, in order to make the enemy give up the idea of launching an attack.[7] In cyberspace, however, it is difficult for either deterrence by punishment or deterrence by denial to fulfill their functions.

Attackers in cyberspace carry out their attacks by using the terminals of a third-party as the jump server, and attempt to escape discovery or identification by disguising these third-party terminals as the source of the attack. The defenders have to analyze these acts of disguise and concealment in order to identify the attackers. To achieve that, it is necessary to obtain various information and carry out analyses, such as the analysis of various communication logs and the terminals used as the jump server, as well as the tracking of the command and control servers that issued the commands to the botnet. However, it takes advanced technology, time, and effort to collect and analyze such information, and it is extremely difficult to identify the attackers. This is what is known as the attribution problem. Even if the defenders were to attempt to carry out a retaliatory attack on the source of the attack, it is difficult to determine if the target is the actual attacker or the third-party used as a jump server. Moreover, it is also difficult to project the effectiveness of the counterattack. Hence, the defenders cannot help but hesitate to execute a retaliatory attack. For this reason, while it is possible for attackers to launch a one-sided attack without fear of reprisal, it is difficult for defenders to identify the source of attack and retaliate. In this sense, it is difficult to strike an overwhelming and unbearable attack on the attackers, making it difficult for deterrence by punishment to function in cyberspace. Vulnerabilities that are caused by software security flaws and which are generally unknown, are called "zero-day vulnerabilities," and it is impossible to completely eliminate such vulnerabilities. Any attempts by the defenders to completely eliminate zero-day vulnerabilities, strengthen security and realize complete defense would incur an infinite cost. While the attackers can select a vulnerability to launch an attack on, it is extremely difficult for the defenders to address and resolve all vulnerabilities. As such, it is also difficult for deterrence by denial to function.

Deterrence through resilience is now drawing attention as a means of overcoming the difficulties of applying the aforementioned conventional theories of deterrence to cyberspace. Deterrence through resilience involves putting in place measures based on the premise of the defender suffering damage as a result of a cyberattack. The approach is to weaken the attacker's will to attack by ensuring that operations continue even when damage has been sustained as

[7] Ministry of Defense, "(Kaisetsu) Yokushi ni Tsuite" [{Explanation} About deterrence], http://www.clearing.mod.go.jp/hakusho_data/2010/2010/html/mc323000.html.

a result of repeated attacks, and that restoration back to the normal status is achieved quickly. Resilience is achieved by estimating the damage based on a detailed risk analysis, drawing up a business continuity plan beforehand according to the respective scenarios, and verifying as well as conducting training and exercises based on these plans, while at the same time, when damage is sustained, ensuring that IT systems continue to operate through means such as migrating to backup systems and enabling fallback operations, maintaining the provision of services at a minimal level, and implementing recovery measures quickly to restore operations to the normal status. The U.S. Department of Defense Cyber Strategy also establishes resilience as a means of deterrence in cyberspace in addition to "response" (deterrence by punishment) and "denial" (deterrence by denial). In addition, it also explains that in order to ensure that resilience functions effectively as a means of deterrence, it is necessary to cooperate with other ministries and agencies, as well as with private-sector actors including CII operators.[8] Efforts by the respective organizational units form the basis of the approach to cyber-resilience; however, when viewed from the perspective of national security, it is effective for the public and private sectors to join hands and for the country to work as one. In order to acquire deterrent capability through resilience, it is important to enhance restoration capacity in the event that damage is sustained in a large-scale cyberattack, through means such as building information-sharing systems for threat information and other data through public-private partnerships, and utilizing cyber exercises as an opportunity for establishing the procedures for measures implemented through public-private partnerships.

(3) The importance of public-private partnerships

As such, from the two perspectives of the characteristics of cyberspace and deterrence, we can see that in cyberspace, unlike the domains of land, sea, air, and space, private-sector actors play an extremely important role. Paradoxically, the more important private-sector actors are in cyberspace, the greater the importance of the role that state leadership fulfills in security in order to unify the direction of efforts by diverse private-sector actors toward ensuring security. In light of the fact that cyberwars are becoming a domain of battle between countries, and that the critical infrastructure of countries have become a perfect target for attacks, governments should not expect private-sector operators to work alone to defend critical infrastructure. For battles in cyberspace, the attackers who have the freedom of selecting the target, means, and timing of the attack, have an overwhelming advantage. To counter the attackers effectively, it is important for the various actors in the public and private sectors to cooperate and work as one to establish a system for coping with attacks, rather than for the defenders to respond individually to attacks.

2. Overview of Public-Private Partnership Systems for Cyber Defense in Japan

(1) Public-private partnership initiatives by the national government

(i) Japan's government-wide security policy promotion system and basic strategy

Japan's security policy was launched in 2000, triggered by the Y2K problem and the continued tampering with and hacking of the websites of central government ministries and agencies,[9] which

---

8 The Department of Defense, *The DoD Cyber Strategy*, (The Department of Defense, 2015), p. 11.

9 JPCERT Coordination Center, "Intanetto Sekyuriti no Rekishi, Dai 5 Kai 'Chuo Shocho Web Peji Kaizan Jiken'" [History of Internet Security, 5th session "Hacking of the websites of central government ministries and agencies"], http://www.jpcert.or.jp/tips/2007/wr071801.html.

occurred immediately after that. The government established the IT Security Office[10] under the auspices of the Cabinet Secretariat to perform the government's core function of implementing information security measures, and also developed a system for promoting government-wide cybersecurity policies. After that, it established the Information Security Policy Council[11] and the National Information Security Center (NISC)[12] in 2005. Furthermore, in January 2015, the Cyber Security Strategy Headquarters was established based on the Basic Act on Cybersecurity, while the former NISC was reorganized as the National center of Incident readiness and Strategy for Cybersecurity (NISC).

The First National Strategy on Information Security was drawn up in 2006 as the basic cybersecurity strategy for the country. This was followed by the Second National Strategy on Information Strategy drawn up in 2009, the Information Security Strategy for Protecting the Nation drawn up in 2010, and the Cybersecurity Strategy drawn up in 2013. The current Cybersecurity Strategy is based on the Basic Act on Cybersecurity enacted in 2014, and was approved by the Cabinet in July 2018.[13]

(ii) Initiatives related to the protection of critical infrastructure

(a) Overall

Information security measures for critical infrastructure began in 2000 when full-scale government-wide initiatives were launched, and the Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure[14] was established. This plan, aimed at protecting critical infrastructure from all attacks that could have a serious impact on citizens' lives and social and economic activities that involve the use of telecommunication networks and information systems, identifies seven relevant categories of critical infrastructure (telecommunications, finance, aviation, railroads, electrical power, gas, and government and administrative services), and prescribes five cyber-terrorism countermeasures that involve public-private cooperation: preventing damage, establishing and enhancing communication and coordination systems between government and the private sector, detection of cyberattacks and emergency response through government and private sector cooperation, establishing foundations of information security, and international cooperation. The Action Plan on Information Security Measures for Critical Infrastructures was approved by the Information Security Policy Council in December 2005, after which the Second Action Plan was approved in 2009, the Third Action Plan was approved in 2014, and the Fourth Action Plan was approved in 2017.

---

10 Cabinet Secretariat, "Jyoho Sekyuriti Taisaku Suishin Kaigi no Secchi ni Tsuite" [Establishment of the IT Security Office], https://www.kantei.go.jp/jp/it/security/suisinkaigi/0229suisinkaigi.html/

11 National center of Incident readiness and Strategy for Cybersecurity (NISC), "Jyoho Sekyuriti Seisaku Kaigi no Secchi ni Tsuite" [Establishment of the Information Security Policy Council], http://www.nisc.go.jp/conference/seisaku/pdf/kitei.pdf.

12 National center of Incident readiness and Strategy for Cybersecurity (NISC), "Jyoho Sekyuriti Senta no Secchi ni Kansuru Kisoku" [Regulations on the Establishment of the Information Security Center], http://www.nisc.go.jp/about/pdf/050420-kisoku.pdf.

13 National center of Incident readiness and Strategy for Cybersecurity (NISC), "Saiba Sekyuriti Senryaku (Heisei 30 Nen 7 Gatsu 27 Nichi)" [Cybersecurity Strategy (July 27, 2018)], http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf.

14 Information Security Measure Promotion Meeting, "Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure," http://www.kantei.go.jp/jp/it/security/taisaku/2000_1215/pdfs/txt3.pdf.

The current Fourth Action Plan on Information Security Measures for Critical Infrastructures[15] sets out 13 fields of critical infrastructure (telecommunications, finance, aviation, railroads, electrical power, gas, government and administrative services, medicine, water, logistics, chemistry, credit, petroleum), and establishes five areas of information security measures to be addressed during the period of the plan. These are: developing safety standards, etc., strengthening information-sharing systems, strengthening failure response systems, establishing risk management and coping mechanisms, and strengthening the protection infrastructure. The respective measures are being promoted.

(b) Information-sharing systems related to the protection of critical infrastructure

In promoting the protection of critical infrastructure, it is extremely important to build a public-private information-sharing system, and to share information related to threats and information security measures. To establish an information-sharing system, the Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure of 2000 prescribed the establishment of Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR) as an organization to fulfill the functions of sharing and analyzing information for CII operators and others.[16] As of the end of September 2017, a total of 18 CEPTOARs are in operation for 13 critical infrastructure domains; industrial organizations and others serve as secretariats, and information is shared between the government and other stakeholders with the aim of preventing service failures for critical infrastructure, preventing the spread of damage, ensuring prompt restoration of services, and preventing recurrence. Furthermore, in order to promote information sharing, the CEPTOAR-Council, comprising representatives of CEPTOARs set up in the respective domains of critical infrastructure, was established in 2009. This Council is engaged in the coordination and management of systems for providing information that is closely related to CII operators and others.[17]

With regard to the flow of information-sharing related to cyberattacks and IT failures, information is shared by the operator in question within the CEPTOAR it is affiliated with. At the same time, the information is also reported to the competent ministries and agencies of the critical infrastructure in question via the CEPTOAR secretariat (or directly), and then disseminated by the CEPTOAR-Council to the CEPTOARs of other fields. The National center of Incident readiness and Strategy for Cybersecurity (NISC) obtains information about failures and other matters related to the critical infrastructure from the competent ministries and agencies of the critical infrastructure (or from the operator in question during an emergency), and shares this information with ministries and agencies involved in disaster risk reduction, case resolution, and information security. It also disseminates the information to business circles outside the field of the critical infrastructure in question.

Alongside with close information-sharing within each CEPTOAR, which are established

---

15 Cybersecurity Strategy Headquarters, "Fourth Action Plan on Information Security Measures for Critical Infrastructures," https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf.

16 Information Security Measure Promotion Meeting, "Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure," http://www.kantei.go.jp/jp/it/security/taisaku/2000_1215/pdfs/txt3.pdf.

17 National center of Incident readiness and Strategy for Cybersecurity (NISC), "Jyoho Kyoyu Taisei no Kyoka" [Strengthening Information-sharing Systems], https://www.nisc.go.jp/active/infra/ shisaku2.html.

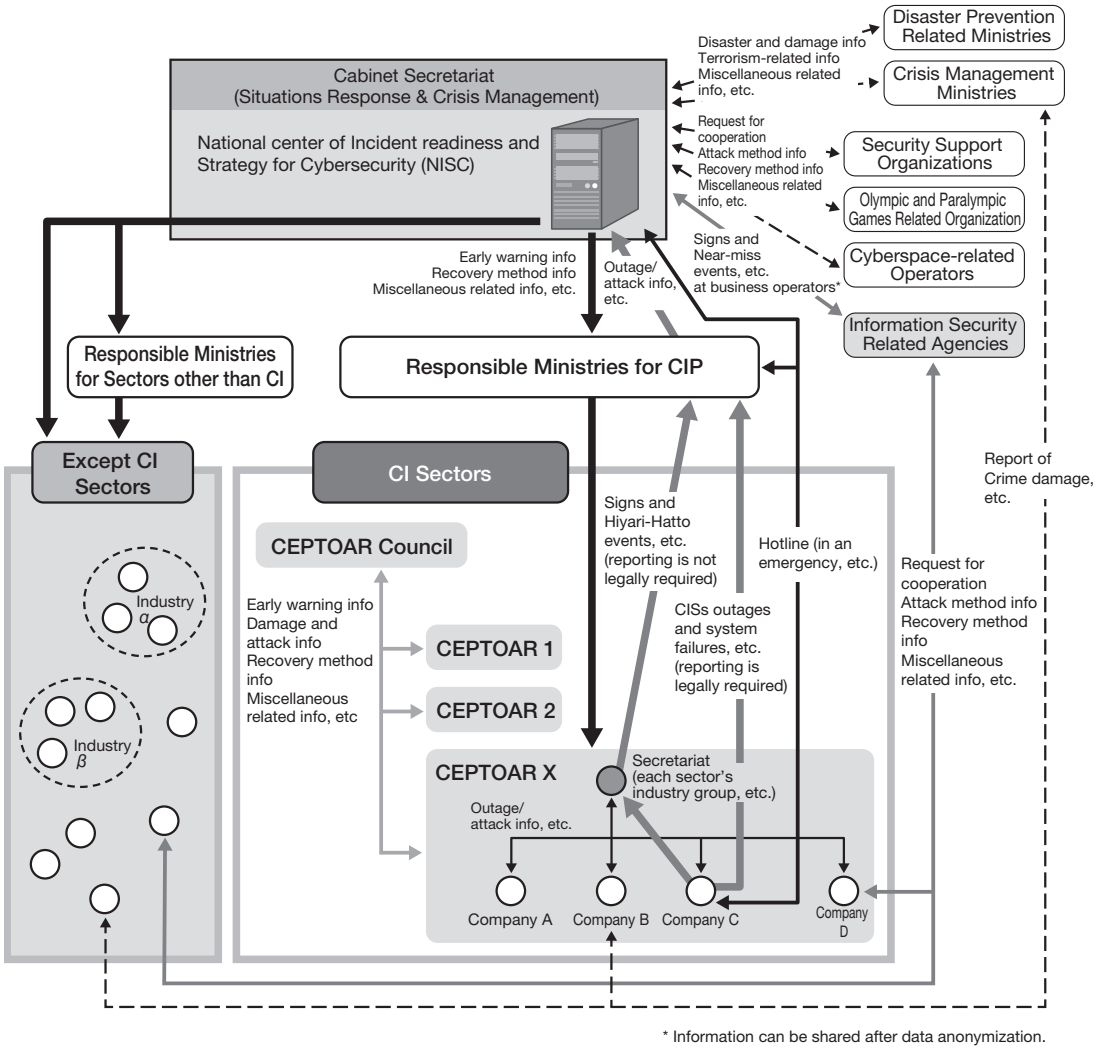
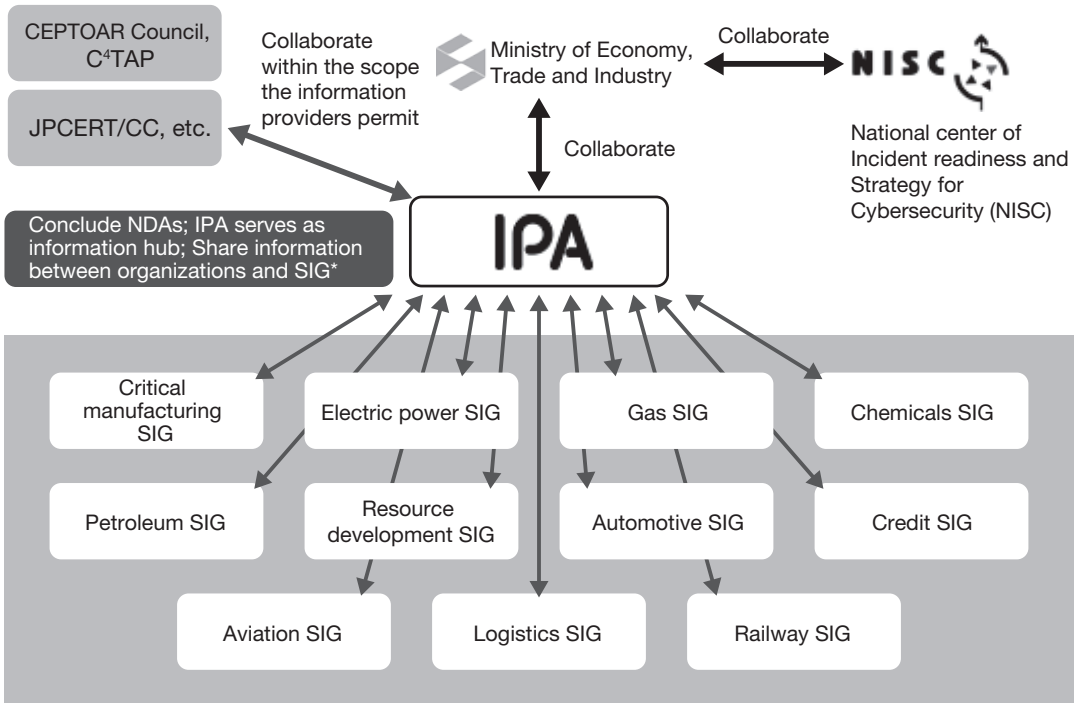


Figure 2 Information-sharing system centered around NISC

Source: Extracted from the Fourth Action Plan on Information Security Measures for Critical Infrastructures

along the lines of the various domains of critical infrastructure, the system is structured such that information is also consolidated by NISC according to the degree of importance and urgency, and disseminated to the relevant organizations.

The Information-technology Promotion Agency (IPA) launched the Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP) in 2011 in cooperation with the Ministry of Economy, Trade and Industry (METI), with the aim of preventing the spread of damage in the event of a cyberattack. This initiative is intended to serve as a space for information-sharing and early response, centered around the manufacturers of equipment used for critical infrastructure. Under the initiative, an information-sharing system has been established by 227 participating organizations, creating 11 Special Interest Groups (SIG, collectives of members from similar industries). IPA has concluded non-disclosure agreements (NDA) with the participating



*SIG: Acronym for "Special Interest Group"

Figure 3 Information-sharing through the Initiative for Cyber Security Information sharing Partnership of Japan

Source: Extracted from the IPA website

organizations, and is engaged in the sharing of information on cyberattacks.[18]

Taking reference from the information Sharing and Analysis Center (ISAC), which is an industry-based information-sharing and analysis organization in the United States, Telecom-ISAC was launched in 2002 primarily for communications carriers, while the Financials ISAC was established in 2014. These organizations share information related to cyberspace in their respective fields.

(C) Implementation status of cross-sectoral exercises

To respond appropriately to IT failures and cyberattacks, it is vital to repeatedly validate the effectiveness of information-sharing systems, emergency response procedures, and business continuity plans, as well as to improve upon them, through exercises and training. From this perspective, cross-sectoral exercises were launched in FY2006 with the aim of improving the functions of public-private partnership systems related to the protection of critical infrastructure. In the inaugural exercise held in FY2006, "research-based exercises" and " tabletop exercises" were held, while annual "functional exercises" have been held since FY2007. The scenarios for the exercises are revised every year, and the difficulty of the scenarios has been raised gradually since

[18] Information-technology Promotion Agency (IPA), Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP), https://www.ipa.go.jp/ security/J-CSIP/.

the launch of the exercises, which have covered coping with a DDoS attack (FY2007), IT failure (FY2008), wide-area power outage (FY2009), large-scale telecommunications failure (FY2010), complex situations involving electricity and gas (FY2011), complex failures of electricity and telecommunications compounded by IT incidents (FY2012), and large-scale information security incidents (FY2013).[19, 20] About 90 representatives from about 10 domains of critical infrastructure participated[21] in the first "tabletop exercise" held in 2006. This has since expanded in scale to participation by about 2,600 people from 13 domains of critical infrastructure[22] at the 12th exercise held in FY2017.

The implementation of cross-sectoral exercises has produced significant results, bringing public- and private-sector stakeholders in public infrastructure together under one roof to conduct verification on the effectiveness of cooperation between the public and private sectors as well as between operators, and at the same time, strengthening response capability within the respective fields by facilitating a common recognition of cross-sectoral threats and understanding of the response situation in other fields, and producing ideas for measures aimed at effective information-sharing between the public and private sectors.

(2) Initiatives by the Ministry of Defense and Self-Defense Forces

The Ministry of Defense, alongside with the National Police Agency, Ministry of Internal Affairs and Communication, Ministry of Economy, Trade and Industry, and Ministry of Foreign Affairs, as members of the Cybersecurity Strategy Headquarters, are engaged in cross-governmental efforts led by the NISC, including participating in exercises on coping with cyberattacks, personnel exchanges, and information-sharing on cyberattacks. In addition, it dispatches personnel to the Cyber incident Mobile Assistance Team (CYMAT), which provides swift and flexible support through cooperation across government ministries and agencies, and contributes in other ways to government-wide initiatives.[23]

As a part of its own initiatives, the Ministry of Defense (MOD) and Self-Defense Forces (SDF) established a new Cyber Defense Group under the SDF Command Control Communication Computers Systems Command in March 2014, through which it operates a 24-hour posture for supporting the information and communications network of the Ministry of Defense and Self-Defense Forces and responding to cyberattacks. The respective Self-Defense Forces also monitor and protect their own information systems through the System Protection Unit of the Ground

---

19 National center of Incident readiness and Strategy for Cybersecurity (NISC), "2013 Nendo Jyuyo Infura no Bunya Odanteki Enshu ni kansuru Chosa no Kekka ni Tsuite" [Results of the Survey on the FY2013 Cross-Sectoral Exercise for Critical Infrastructure], https://www.nisc.go.jp/active/infra/pdf/bunyaoudan_2013.pdf.

20 National center of Incident readiness and Strategy for Cybersecurity (NISC), "Jyuyo Infura ni okeru Bunya Odanteki Enshu – [CIIREX 2010] no Jisshi ni Tsuite" [Cross-Sectoral Exercises for Critical Infrastructure – Implementation of CIIREX 2010], https://www.nisc.go.jp/press/pdf/ciirex2010_press.pdf.

21 National center of Incident readiness and Strategy for Cybersecurity (NISC), "2010 Nendo Jyuyo Infura no Bunya Odanteki Enshu ni kansuru Chosa no Kekka ni Tsuite" [Results of the Survey on the FY2010 Cross-Sectoral Exercise for Critical Infrastructure], https://www.nisc.go.jp/active/infra/pdf/bunyaoudan_2010.pdf.

22 National center of Incident readiness and Strategy for Cybersecurity (NISC), "Jyuyo Infura 13 Bunya wo Taisho ni Sabisu Shogai Taio no tame no Saiba Enshu wo Jisshi – 2017 Nendo Bunya Odanteki Enshu" [Implementation of Cyber Exercises for Responding to Service Outages in the 13 Critical Infrastructure Domains – FY2017 Cross-Sectoral Exercise], http://www.nisc.go.jp/active/infra/pdf/bunya_enshu2017gaiyou.pdf.

23 Ministry of Defense, *Defense of Japan 2017*, (Nikkei Printing Inc., 2017), p. 359.

Self-Defense Force, the Communication Security Group of the Maritime Self-Defense Force, and the Computer Security Evaluation Squadron of the Air Self-Defense Force. The MOD and SDF are working to enhance systems, including improving military facility to withstand attacks, strengthening information-gathering as well as research and analysis functions, and developing a training environment for actual combat, so as to cope effectively with cyberattacks on their information systems and networks.[24]

As for international initiatives, the MOD and SDF have established the Cyber Defense Policy Working Group (CDPWG) in partnership with Japan's ally, the United States, and hold conferences on topics such as promoting policy consultation, facilitating closer information-sharing, promoting joint exercises, and cooperating to develop and secure experts. They also engage in exchanges of opinions with countries such as the UK, Australia, and Estonia through the establishment of cyber-consultations among the defense authorities. At the same time, they have cooperated with NATO to set up NATO-Japan Cyber Defense Staff Talks, and are engaged in other efforts to build up its cooperative relationship with NATO, such as by participating as an observer in Cyber Coalition, Locked Shields and other cyber defense exercises organized by NATO.

In Japan, efforts are underway to improve the ability of the MOD and SDF, as well as the defense industry, to cope with cyberattacks, through initiatives such as joint exercises, and the establishment of the Cyber Defense Council in 2013, comprising about 10 companies with a deep interest in cyber security as its core members.[25]

(3) Summary

Japan's cybersecurity measures were launched in response to the Y2K problem. To date, a wide range of measures have been implemented steadily in the areas of governmental organizations, strategy formulation, and development of legal systems. These include the establishment of the Cybersecurity Strategy Headquarters and the National center of Incident readiness and Strategy for Cybersecurity, the formulation of cybersecurity strategies, and the enforcement of the Basic Act on Cybersecurity. With regard to initiatives related to the protection of critical infrastructure, it has also strengthened public-private partnership systems based on the respective action plans, through the establishment of information-sharing systems and cross-sectoral exercises. The MOD and SDF have established new dedicated cyber defense units and cooperated with the government as a whole on various initiatives, while at the same time building international cooperative relationships with allies and friendly countries such as the United States.

3. Estonia's Initiatives, Comparison with Japan, and Feasibility of Implementation in Japan

Since it gained independence from the Soviet Union in 1991, Estonia has advanced efforts to utilize information and communications technology at the national level with a view to realizing an e-government. The Estonian government has decided to concentrate its resources on information and communications technology in order to achieve economic growth in an efficient manner, in light of the country's limited natural resources. This approach is supported by the citizens. As the country needed to develop social infrastructure such as roads and schools in the early stages

[24] Ministry of Defense, "Jieitai no Saiba Kogeki e no Taio ni Tsuite" [SDF's Response to Cyberattacks], http://www.mod.go.jp/j/publication/net/shiritai/cyber/index.html#a2.

[25] Ministry of Defense, *Defense of Japan 2017*, p. 361.

of its independence, it poured its efforts into creating an environment for using the Internet. It has even been said that the introduction of computers was prioritized over the repair of roofs in schools.[26] From 1996 to 2000, it implemented the "Tiigrihüpe" ("Tiger Leap") project with the aim of overtaking developed countries through the use of information and communications technology. In addition to building environments to enable Internet use in all schools, it also promoted the use of the Internet across a wide range of public services and banking processes. In 2001, it built X-Road, a data exchange layer that serves as an information and communications infrastructure for governmental organizations, thereby enhancing efficiency in the exchange and sharing of information among government ministries and agencies. The eID card, which forms the basis for personal authentication and electronic signature, has been distributed to all citizens aged 15 and above since 2002. In 2005, Estonia became the first in the world to conduct local government elections through electronic voting on the Internet.[27] As a result of such intensive investment in information and communications technology, Estonia's global ranking for the penetration of information and communications technology rose from 33rd place in 1999[28] to 17th place in 2017.[29] (Estonia comes second after the Republic of Korea in the rate of increase of its ranking during this period of time.)

Against this background, Estonia was hit by a large-scale cyberattack on its critical infrastructure in April 2007. Drawing lessons from this incident, Estonia has taken strong steps to promote cybersecurity initiatives, and the various measures it has put in place are exceedingly advanced even among the NATO member countries. The Global Cybersecurity Index (GCI) 2017 report published by the International Telecommunication Union (ITU) positioned Estonia in the fifth place globally among 193 countries, and first in the Europe region.[30] (The GCI assesses countries based on the five pillars of legal measures, technical measures, organizational measures, capacity building, and cooperation. Globally, Singapore ranks first, the United States ranks second, and Japan ranks 11th.) In this GCI report, Estonia was highly rated for its efforts after the large-scale cyberattack of 2007 to develop its legal system so as to ensure the provision of a minimal level of services even when the Internet is shutdown, and to promote organizational measures for swift response to attacks.[31]

Estonia has also established a Cyber Command in its regular military forces, as well as a Cyber Defense Unit comprising volunteers from the private sector under the auspices of the Estonian Defense League, a paramilitary organization. With regard to national defense against cyberattacks, the country has developed a unique military-civilian partnership system that is not seen in any other country. Based on these facts, we can see that Estonia is a democracy that has put nationwide efforts toward the realization of an e-government through the use of the Internet,

---

26 Allikivi, Raul, and Yoji, Maeda, *Miraigata Kokka Estonia no Chosen – Denshi Seifu ga Hiraku Sekai* [Challenges Faced by the Future-Oriented State of Estonia – Opening Up a New World Through e-Government], (Impress R&D, 2016)

27 Ibid., pp. 52-53.

28 United Nations Conference on Trade and Development, *Information and Communication Technology (ICT) Development Indices*, (Geneva, UNCTAD Secretariat, 2003), p. 44.

29 International Telecommunication Union, *Measuring the Information Society Report 2017 Volume1*, (Geneva, ITU, 2017), p. 31.

30 International Telecommunications Union, *Global Cybersecurity Index (GCI) 2017*, p. 17.

31 Ibid., p. 36.

as well as a country that fell victim to a large-scale cyberattack that had a severe impact on the critical infrastructure of the country. It has strongly promoted various measures based on the lessons drawn, placing the focus of its cyber defense system on public-private and military-civilian partnerships rather than on the military and bureaucracy, and has been successful in developed a national cybersecurity system.

The population of Estonia is about 1.32 million, which is approximately one-hundredth of the population of Japan. From the perspective of national scale, there may be critics who feel that Estonia is not an appropriate subject in drawing a comparison of the cybersecurity policies with Japan. However, Estonia enjoys the merits of having few stakeholders who hold a stake, as well as ease of promoting new measures, because it is a country with a small population. It has taken advantage of these precise merits to promote e-government measures, and at the same time, advanced new cybersecurity policies. As these leading initiatives that take advantage of the merits of being a small country offer many implications, such as examples of successes as well as failed measures, they can be fully utilized when considering future initiatives for Japan's cybersecurity measures.

This section looks at Estonia's cyber defense initiatives, placing particular focus on public-private partnership in the protection of critical infrastructure, and provides an overview of the various measures based on the following six classifications: cybersecurity strategy, legal systems, public-private partnership organizations and information sharing systems, risk analysis and business continuity plans, cyber exercises, and national defense strategy and organizations. It carries out a comparison with Japan, and discusses the feasibility of implementing these measures in Japan.

In Estonia's laws and strategy documents, "vital service" is a term used in relation to the protection of critical infrastructure. Hence, in deference to the usage of the term in Estonia, this section will apply the term "vital service" in regard to the protection of critical infrastructure in Estonia.

(1) Cybersecurity strategy

(i) Estonia's national security strategy and cybersecurity strategy

The most important document related to Estonia's national security is the National Security Concept of Estonia, which was revised in 2010 base on lessons drawn from the large-scale cyberattack of 2007.[32, 33] With regard to the environment in Estonia, information and communications systems are becoming increasingly important in society, and vital services are also becoming increasingly dependent on information and communications systems; hence, a vital service outage will have severe impact on society. In light of this, the National Security Concept points to the importance of ensuring the security of information and communications systems, and positions the securing of

[32] Christian Czosseck, Rain Ottis and Anna-Maria Taliharm, Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security, (NATO CCD COE), p. 59. http://ccdcoe.org/articles/2011/Czosseck_Ottis_Taliharm_Estonia_After_the_2007_Cyber_Attacks.PDF

[33] Estonia published its revised National Security Concept of Estonia 2017 in October 2018 after this paper was written. http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017.pdf.

resilience for vital services as one of the important elements of national defense.[34] Furthermore, it also clearly sets out measures aimed at securing the resilience of vital services, including improving restoration capacity when damage is incurred, prior preparation of reserve supplies, formulation of action plans, and continued evaluation of risk analysis.[35]

After the large-scale cyberattack of 2007, the Estonian Ministry of Defense established the Cyber Security Strategy Committee through cooperation between the Ministry of Education and Research, Ministry of Justice, Ministry of Economic Affairs and Communications, Ministry of the Interior, and Ministry of Foreign Affairs, and promoted the formulation of a national Cyber Security Strategy. In May 2008, Cyber Security Strategy 2008 – 2013 was drawn up.[36] In 2011, the authority for the inter-agency coordination of cybersecurity policies was transferred from the Ministry of Defense to the Ministry of Economic Affairs and Communications, and the responsibility of preparing the cybersecurity policies of Estonia fell to the Ministry of Economic Affairs and Communications its subordinate organization, the Estonian Information System Authority ("Riigi Infosüsteemi Amet" or RIA. Discussed in detail later.)

The current Cyber Security Strategy is the Cyber Security Strategy 2014 – 2017, published by the Estonian Ministry of Economic Affairs and Communications, and it is positioned as the basic document covering cybersecurity in Estonia. This Strategy is structured as follows: Chapter 1: Analysis of current situation (Sectoral progress; Trends; Challenges), Chapter 2: Principles of ensuring cyber security, Chapter 3: General objective of the strategy for 2017; Chapter 4: Subgoals; Chapter 5: Parties related to the strategy. It places focus on the areas of maintaining vital services, effective response to cybercrimes, and progress of national defense capability.[37] The main goal of this Strategy is to secure safety in cyberspace by enhancing cybersecurity capability and raising awareness of cyber threats among the population.[38] This Strategy then sets out five subgoals for achieving the main goal: ensuring the protection of information systems underlying important services; enhancing of the fight against cybercrime; development of national cyber defence capabilities; managing evolving cyber security threats; and, developing cross-sectoral activities.[39]

The Cyber Security Strategy is characterized by the fact that it positions "Ensuring the protection of information systems underlying important services" as the issue of the highest priority. The Strategy lays out the following measures for achieving this subgoal: ensuring alternative solutions for important services, managing cross-dependency between important services, ensuring the security of ICT infrastructure and services, managing cyber threats to the public and private sector, introducing a national monitoring system for cyber security, ensuring digital continuity of the state, and promoting international cooperation in the protection of the infrastructure of critical information.

---

34 Parliament of Estonia, *National Security Concept of Estonia*, May 12, 2010, pp. 13-14. http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_of_estonia.pdf

35 Ibid., p. 17.

36 Tikk, *International Cyber Incidents: Legal Consideration*, pp. 29-30.

37 Ministry of Economic Affairs and Communication, *Cyber Security Strategy 2014-2017*, 2014, p. 6.

38 Ibid., p. 8.

39 Ibid., p. 8.

(ii) Comparison with Japan's cybersecurity strategy

Comparing Estonia's Cyber Security Strategy 2014 – 2017 and Japan's Cybersecurity Strategy (approved by the Cabinet in July 2018), we can see that the two countries are generally in accord with regard to their recognition of the threats facing cyberspace, recognition of the benefits that cyberspace has given to society, and the aims and goals of the respective cybersecurity strategies. However, the two countries differ from the perspective of the priority they place on measures related to the protection of critical infrastructure.

Japan's Cybersecurity Strategy establishes the promotion of cybersecurity that underpins the creation of new values as the first measure within the four policy approaches (Enabling socio-economic vitality and sustainable development; Building a safe and secure society for the people; Contribution to the peace and stability of the international community and Japan's national security; Cross-cutting approaches to cybersecurity), and places the emphasis on enhancing socio-economic vitality and sustainable development in Japan alongside with the growing and widespread use of IoT systems.[40]

While Estonia's Cyber Security Strategy places "Ensuring the protection of information systems underlying important services" as the issue of top priority in the Cyber Security Strategy, Japan's Cybersecurity Strategy positions the protection of critical infrastructure as the fifth initiative[41] out of a total of 16 measures, and covers it alongside with other measures. It may be argued that the order of the measures set out in Japan's Cybersecurity Strategy does not reflect their degree of importance. However, we could say that Estonia differs greatly from Japan in that it clearly positions the protection of vital services as the top priority, and has established the protection of vital services at the center of its approach to cybersecurity.

Table 1 Comparison of cybersecurity strategies of Estonia and Japan

	Estonia	Japan
Most important issues	1. Ensuring the protection of information systems underlying important services 2. Enhancing of the fight against cybercrime 3. Development of national cyber defence capabilities 4. Managing evolving cyber security threats 5. Developing cross-sectoral activities	1. Enabling socio-economic vitality and sustainable development 2. Building a safe and secure society for the people 3. Contribution to the peace and stability of the international community and Japan's national security 4. Cross-cutting approaches to cybersecurity
Protection of critical infrastructure	Positioned as first item among five subgoals (first item among 22 measures)	Positioned as second item among four policy approaches (fifth item among 16 measures)
Order of priority for each measure	Description corresponding to degree of priority (explicit)	Description alongside with other policy approaches (not explicit)

Source: Drawn up based on the cybersecurity strategies of Estonia and Japan

40 *Cybersecurity Strategy*, approved by the Cabinet on July 27, 2018, pp. 13-42.

41 Ibid., pp. 13-42.

(iii) Feasibility of implementation in Japan

The formulation of Japan's Cybersecurity Strategy is mandatory in accordance with the provisions of Article 12 of the Basic Act on Cybersecurity, and the Strategy is drafted by the Cybersecurity Strategy Headquarters. While there are no specific provisions stipulating the contents to be included in the Cybersecurity Strategy, it is possible to explicitly set out the order of priority for the respective policy approaches in the same way as Estonia's Cyber Security Strategy.

The viewpoint of actively using cyberspace as a means for economic development is an important one. However, cyberspace is established through the maintenance of networks by communications carriers and a stable supply of electricity that underpins that. Accordingly, we could say that economic development based on the use of cyberspace is first realized through the stable operation of the country's critical infrastructure. As indicated by Estonia's Cyber Security Strategy, Japan's Cybersecurity Strategy should also position measures to protect critical infrastructure from large-scale cyberattacks as the issue of the highest priority.

(2) Legal systems

(i) Legal systems related to the protection of vital services in Estonia

In Estonia, there are no specific laws for cybersecurity like Japan's Basic Act on Cybersecurity.[42] Instead, the protection of vital services is clearly provided for under the Emergency Act. This Act, revised in 2009, clearly sets out 43 types of vital services and the competent ministries and agencies for these services.[43] The number of vital services, which far exceeds the 13 domains of critical infrastructure established by Japan, is due to the detailed categorization and listing of the respective vital services in Estonia, and there are many vital services in Estonia's list that have not been defined as critical infrastructure in Japan. (For example, ports, shipping traffic, roads, emergency aid messages, and environmental monitoring of radiation, atmosphere and oceans, to state a few.)

At the Cybersecurity Conference organized by the Estonian Information System Authority ("Riigi Infosüsteemi Amet" or RIA) in 2013, vital service providers were of the view that it is necessary to develop a clearly defined legal system for regulation corporations, such as the actions that vital service providers should take when a large-scale cyberattack occurs, and the minimum level of services that should be maintained by vital service providers in order to sustain social life in the event of an emergency. To that end, they recommended revision to the law. Consequently, the Emergency Act was revised in July 2017 and vital services were organized into 14 categories (electricity supply, gas supply, fuel supply, national roads, fixed-line telephones, mobile phones, data transmission services, digital identification and digital signing, emergency care, payment services, cash circulation, district heating, local roads, and water supply and sewage). At the same time, the responsibilities of the competent ministries and agencies as well as of the vital service providers were clearly defined.[44]

---

[42] Estonia enacted the Cybersecurity Act in May 2018, after this paper was written. Government of Estonia, Emergency Act passed 09.05.2018. https://www.riigiteataja.ee/en/eli/523052018003/consolide.

[43] Government of Estonia, *Emergency Act passed 15.06.2009, Art.34*, https://www.riigiteataja.ee/en/eli/525062014011/consolide.

[44] Government of Estonia, *Emergency Act passed 08.02.2017, Art.36*, https://www.riigiteataja.ee/en/eli/513062017001/consolide.

Article 38 of the Emergency Act sets out the following responsibilities of vital service providers: (1) Prepare the continuity risk assessment and plan of the vital service; (2) Implement measures that prevent interruptions of vital services; (3) Ensure the capability to guarantee the continuity of and to quickly restore the services; (4) Notify the authority organizing the continuity of the vital service in the event of an emergency; (5) Participate in resolving an emergency according to the emergency response plan; (6) Provide information to the competent authority and other relevant parties; (7) Organize exercises in order to verify the continuity of the vital service ; and others. Furthermore, Article 37 of the same law sets out the following responsibilities of the competent ministries and agencies of vital services: (1) Coordinate the ensuring of the continuity of the vital service; (2) Advise providers of vital services; (3) Exercise supervision over ensuring the continuity of vital services; (4) Approve the continuity risk analyses and plans of providers of vital services; (5) Coordinate the resolution of an emergency; (6) Prepare an emergency response plan; and others. It also clearly sets out the continuity requirements that the competent ministries and agencies demand of vital service providers in relation to the continuity of their vital service operations: (1) The contents of the vital services for which functions should be maintained; (2) Service levels that should be maintained; (3) Requirements for the prevention of interruption; (4) Time permitted for interruption; (5) Service failures that constitute an emergency; (6) Reporting when an emergency arises; and others.

(ii) Comparison with Japan's legal system

Japan's Basic Act on Cybersecurity sets out in Article 3 (Basic Principles) that "the promotion of the Cybersecurity policy must be carried out with the intent to produce active responses to threats against Cybersecurity through coordination among multiple stakeholders, including the national government, local governments, and critical information infrastructure (CII) Operators," and in Article 6 (Responsibility of CII Operators) that "In accordance with the Basic Principles and for the purpose of stable and appropriate provision of their services, CII Operators are to make an effort to: deepen their awareness and understanding of the critical value of Cybersecurity; ensure Cybersecurity voluntarily and proactively; and cooperate with the measures on Cybersecurity taken by the national government or local governments." Hence, the law only provides for efforts to cooperate with measures set out by the government. For this reason, although NISC promotes various measures by positioning the Action Plan on Information Security Measures for Critical Infrastructures as the basic document for information security measures related to critical infrastructure, CII operators are not legally obligated (legal duty) to be involved in these measures based on the Basic Act on Cybersecurity.

Estonia's Emergency Act clearly sets out the responsibilities of vital service providers, including risk analysis and formulation of business continuity plans, measures to prevent interruption to vital services, and reporting in the event of an emergency. It differs from Japan in the sense that it imposes a certain degree of legal duty on vital service providers to ensure cybersecurity. Moreover, there is a sense that vital service providers who are regulated by law are more involved in the enactment of legislation for vital service providers, such as criticizing the government for inadequacies in the Emergency Act and promoting revisions to the law.

Table 2 Comparison of legal systems of Estonia and Japan47

	Estonia	Japan
Legal framework	• Provided for in the Emergency Act * Discussions are ongoing about the need for a basic law on cybersecurity[45]	• Basic Act on Cybersecurity • Laws regulating the respective industries, etc.
Responsibilities of CII operators	• Prepare risk analysis and business continuity plan • Implement measures that prevent interruptions of vital services • Ensure the capability to ensure the continuity, etc. • Notify the competent authorities in the event of an emergency • Participate in resolving an emergency according to the emergency response plan • Provide information to the competent authority • Organize exercises to verify the business continuity plans	• Voluntarily and proactively put effort into ensuring cybersecurity • Cooperate on cybersecurity measures implemented by the government and other entities
Responsibilities of the government and competent ministries and agencies	• Coordinate the ensuring of the continuity of the vital service • Advise providers of vital services • Exercise supervision over ensuring the continuity of vital services • Approve the continuity risk analyses and plans • Coordinate the resolution of an emergency • Prepare an emergency response plan	• Promotion of the establishment of standards, exercises and training, sharing of information, and other voluntary initiatives related to cybersecurity by CII operators, as well as the implementation of other necessary measures.

Source: Drawn up based on Estonia's Emergency Act and Japan's Basic Act on Cybersecurity

(iii) Feasibility of implementation in Japan

With regard to regulations based on laws for ensuring the security of critical infrastructure, in addition to the Basic Act on Cybersecurity, it is possible to reexamine the regulations through revision to the laws governing the respective industries, which are under the jurisdiction of each competent ministry and agency of the critical infrastructure. As for the implementation of cybersecurity policies, strengthening regulations on all matters through the application of the law could hinder free and flexible activities by corporations, and may not necessarily be the right thing to do. In particular, the frameworks for sharing of information between the public and private sectors in Japan have developed without the enforcement of any legally binding force. Hence, it is not necessary to re-establish systems based on law to regulate such mature systems that have developed through voluntary efforts.

However, there is a need to develop law-based systems to mandate the implementation of risk analyses and formulation of business continuity plans by CII operators, so as to provide assurance for matters that form the foundation of the protection of critical infrastructure that could have a severe impact on citizens' lives and socio-economic activities, or in other words, to ensure the provision of the minimal level of services in the event of critical infrastructure outage, as well as to ensure the swift restoration of services when operations are interrupted.

45 The Cybersecurity Act was enacted in May 2018 after this paper was written.

(3) Public-private partnership organizations and information-sharing systems

(i) Estonia's public-private partnership organizations and information-sharing system

In 2009, the Cyber Security Council was added to the Security Committee of the Estonian government. It was tasked with promoting strategic cooperation between the ministries and agencies, and carrying out supervision to ensure that the goals set out in the Cyber Security Strategy were achieved. In 2010, the responsibility of formulating cybersecurity policies, which had until then been the job of the Ministry of Defense, was transferred to the Ministry of Economic Affairs and Communications. Alongside with this, the Estonian Information System Authority ("Riigi Infosüsteemi Amet" or RIA) was established as the agency responsible for the implementation of Estonia's cybersecurity policies.

The primary duties of the RIA[46] are as follows:

- To monitor the information systems of vital services and implement security measures
- To engage in organizational security activities on information systems of governmental organizations and critical infrastructure
- To deal with security incidents affecting computer networks in Estonia
- To supervise the situation of compliance with the standards of security measures for the information systems of governmental organizations
- To maintain and manage the information systems of governmental organizations and the information and communications infrastructure (X-Road)
- To carry out coordination in relation to maintaining the functions of the public key infrastructure (PKI)
- To carry out coordination in relation to the development of information systems for governmental organizations and participation in international projects
- To participate in the activities of the European Union (EU)
- To participate in various activities pertaining to the legal systems, policies, strategies, and development in relation to cybersecurity

RIA, in comparison with its predecessor, the former Estonian Informatics Center, has greater authority over the protection of the country's information and communications infrastructure, and is also responsible for supervision to ensure that information systems related to vital services are secure.[47] The Critical Information Infrastructure Protection (CIIP) is established within the RIA with the aim of protecting vital services. It is responsible for the protection of public and private information systems that are related to the maintenance of the functions of vital services.[48] CIIP is the main department in RIA that conducts general risk evaluation in relation to vital services, as well as formulates national emergency response plans in preparation for the event of a large-scale cyber incident. In 2010, it conducted a mutual dependency survey for vital services, and clearly established the security requirements for the critical information systems that are necessary for the country to function.[49] The supervision of all services in the respective fields of vital services comes under the charge of the competent ministries and agencies for the vital services, as before.

---

46 Information System Authority, https://www.ria.ee/en/about-estonian-information-system-authority.html.

47 Government of Estonia, *Status of the Information System Authority, Art.8*, https://www.ria.ee/public/RIA/Dokumendid/Statutes_of_RIA.pdf.

48 Critical Information Infrastructure Protection, https://www.ria.ee/en/ciip.html.

49 Ministry of Economic Affairs and Communication, Cyber Security Strategy 2014-2017, 2014, p. 2.

However, matters related to ensuring cybersecurity for information systems that make up the vital services are directly supervised by RIA. This system makes is possible to consolidate the various information on the information infrastructure that supports vital services, which had previously been scattered across the competent ministries and agencies, under the CIIP of RIA, making it possible to effectively and efficiently perform tasks that are related to the identification and supervision of vital service providers who are lagging behind in the implementation of security measures.

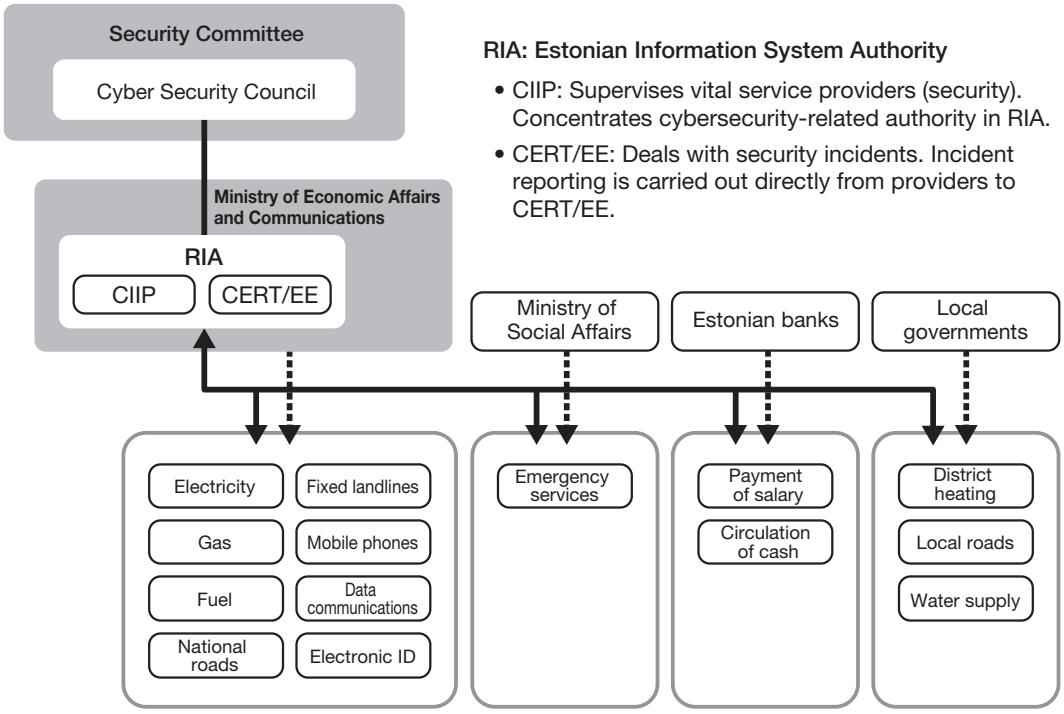


Figure 4 Relationship between RIA, the competent ministries and agencies of vital services, and vital service providers

Source: Drawn up based on the RIA website and the Emergency Act

With regard to the information-sharing system, the Estonian Computer Emergency Response Team (CERT-EE) is established within the RIA. Its scope of work includes incident handling for information systems related to vital services, notification of alert information, and providing support for the relevant organizations. The Security Measures for Information Systems of Vital Services and Related Information Assets[50] prescribes, as one of the enforcement rules of the Emergency Act, that in the event of a serious security incident, vital service providers are required to notify RIA and report on post-incident measures.

[50] Republic of Estonia Information System Authority, *Security measures for information systems of vital services and related information assets*, https://www.ria.ee/public/KIIK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf.

(ii) Comparison with Japan's public-private partnership organizations and information-sharing systems

With regard to public-private partnership organizations, Japan's core organization is the NISC. Its responsibilities[51] are as follows:

- Monitoring and analysis of illegal activities on the information systems of all administrative departments
- Investigations to uncover the cause of serious events that could impede efforts to ensure cybersecurity in all administrative departments
- Offering the necessary advice, information, and other forms of assistance for ensuring cybersecurity in all administrative departments
- Carrying out the necessary audits in relation to ensuring cybersecurity in all administrative departments
- Other administrative work pertaining to the planning, drafting, and overall coordination needed for the standardized maintenance of measures for all administrative departments, in relation to ensuring cybersecurity

Table 3 Comparison of the public-private partnership organizations and information-sharing approaches of Estonia and Japan

	Estonia	Japan
Public-private partnership promotion organizations	Estonian Information System Authority ("Riigi Infosüsteemi Amet" or RIA), under the Ministry of Economic Affairs and Communications	National center of Incident readiness and Strategy for Cybersecurity (NISC)
Supervision of CII operators	Has direct supervision authority (Only for areas related to ensuring security)	Does not have supervision authority (Advice and overall coordination of competent ministries and agencies)
Responsibilities	• To monitor the information systems of vital services • To engage in organizational security activities on information systems of governmental organizations and critical infrastructure • To deal with security incidents • To supervise the situation of compliance with the standards of security measures for the information systems of governmental organizations • To maintain and manage the information systems of governmental organizations • To maintaining the functions of the public key infrastructure (PKI) • To participate in international projects and EU activities • To participate in various activities pertaining to the legal systems, policies, strategies, and development in relation to cybersecurity	• Monitoring and analysis of illegal activities on the information systems of all administrative departments • Investigations to uncover the cause of serious events that could impede efforts to ensure cybersecurity in all administrative departments • Offering the necessary advice, information, etc. for ensuring cybersecurity in all administrative departments • Carrying out the necessary audits in relation to ensuring cybersecurity in all administrative departments • Other administrative work pertaining to the planning, drafting, and overall coordination needed for the standardized maintenance of measures for all administrative departments, in relation to ensuring cybersecurity

Source: Drawn up based on the RIA website and the Order for the Organization of the Cabinet Secretariat

[51] National center of Incident readiness and Strategy for Cybersecurity (NISC), "Order for the Organization of the Cabinet Secretariat (Order No. 219 of 1957)," http://www.nisc.go.jp/law/pdf/soshikirei.pdf

As described above, NISC is engaged in planning and drafting work related to ensuring cybersecurity, and promotes measures through the overall coordination of the competent ministries and agencies of critical infrastructure. Under this system, the competent ministries and agencies of the respective critical infrastructure supervise CII operators based on the laws that govern the respective sectors.

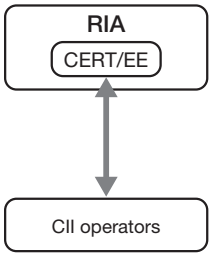
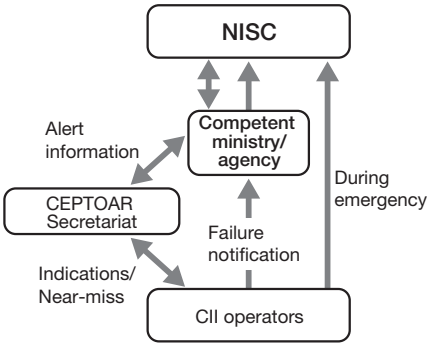
Comparing Japan's NISC and Estonia's RIA, we can see a significant difference in the sense that RIA has the authority to supervise vital service providers with regard to information systems, while NISC does not have direct authority to supervise CII operators.

With regard to the information-sharing systems, Japan has established a CEPTOAR for each domains of critical infrastructure to fulfill the functions of sharing and analyzing information in each of the domains. In contrast, Estonia does not have an organization for information-sharing and analysis for each domain of vital services; instead, this function is served primarily through the direct relationship between RIA and vital service providers. In Japan, as there are many corporations within each domain of critical infrastructure, there is a mature information-sharing and cooperation relationship between corporations within each CEPTOAR, followed by the maturing of the cooperative relationship between the public sector and the CEPTOARs. In Estonia, a country that is much smaller than Japan, there is a limited number of corporations for each domain of vital services. As such, the direct relationship between the public sector and corporations is considered to be mature.

As for information-sharing in the event of a security incident, in the case of Japan, CII operators notify NISC via the CEPTOAR Secretariat and the competent ministry or agency of the critical infrastructure. In the case of Estonia, however, the vital service providers notify CERT-EE under the RIA directly. Estonia surpasses Japan in the aspects of the volume of incident information that CERT has acquired and accumulated, as well as the need to report speedily.

Furthermore, the reporting of security incidents is mandated by law in Estonia, and companies cannot hesitate in making reports for fear that doing so may have a negative impact on their corporate image.

Table 4 Comparison of information-sharing systems of Estonia and Japan

	Estonia	Japan
Information-sharing system		

Source: Drawn up based on the RIA website and NISC website

(iii) Feasibility of implementation in Japan

It is necessary to resolve various issues of Japan's NISC is to take on the function of directly supervising CII operators on the implementation of cybersecurity policies in the same way as Estonia's RIA. Firstly, the supervision of all CII operators is difficult based on the current personnel strength in NISC. Hence, there is a need to either increase the number of personnel assigned to NISC, or to use other means such as outsourcing the work to a third-party organization. In addition, it will probably also be necessary to segregate work related to the field of cybersecurity, from among the tasks of supervising CII operators that the respective competent ministries and agencies of the respective critical infrastructure are responsible for.

With regard to the information-sharing systems, as there is a very large number of companies in each critical infrastructure domain in Japan as compared to Estonia, it would be difficult for the NISC to process the overwhelming volume of incident information if CII operators were to report directly to NISC. Hence, it would probably be preferable to maintain the current system of using CEPTOARs for each sector.

(4) Risk Analysis and Business Continuity Plans

(i) Estonia's risk analysis and business continuity plans for vital services

Drawing up a risk analysis for vital service outages and business continuity plans for service interruptions in advance is extremely important for the implementation of the necessary measures beforehand, as well as for the smooth implementation of restoration work in the event that damage is incurred. In Estonia, vital service operators are mandated under the Emergency Act to draw up risk analysis and business continuity plans for vital services, while the procedures for the formulation of these documents and their contents are prescribed by the Ministry of the Interior regulation, "Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan."[52] Upon its designation as a vital service provider, the business operator in question is required to conduct a risk analysis, formulate a business continuity plan, and submit these to the competent ministry or agency within a year. Risk analyses and business continuity plans must be updated at least once every two years, and every time there are significant changes to the threats or environment surrounding the vital services. When it is deemed unnecessary to change the contents of a previous risk analysis and business continuity plan based on the results of an analysis conducted for the update of the documents, the vital service provider is required to notify the competent ministry or agency.

Risk analyses are implemented in five stages. The first stage is to clarify why the service in question has been designated as a vital service, and to define who the users of the service are, the number of users, the service coverage area, minimum service provision level in the event of an emergency, and maximum tolerable period of disruption during an incident. The second stage is to identify the critical activities necessary for the vital service to function, and to analyze the degree of importance of these activities. It also involves the analysis of the resources necessary for the critical activities (staff, buildings and territory, IT, information, funds, other services, suppliers and collaborators). The third stage is to identify the threats that may impede the critical activities,

---

[52] Minister of the Interior, *Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan*, https://www.riigiteataja.ee/en/ eli/525092017001/ consolide.

identify multiple scenarios that could bring about a loss in the functions of the vital service, evaluate the likelihood of occurrence of the scenario (five-grade evaluation) and the extent of damage accompanying the occurrence of the scenario (five-grade evaluation), and calculate the class of risk (five-grade evaluation). The fourth stage is to analyze, in the event of the occurrence of the scenarios, the measures that should be implemented at the current point in time and the measures that should be implemented in order to reach the standards of maintaining the minimum service levels and the standards of maximum tolerable period of disruption within three years. Finally, to summarize the risk analysis, the fifth stage involves summarizing the instructions pertaining to: (1) List of order of priority for the critical activities; (2) List of scenarios ranked high for the class of risk; (3) Threats that have the potential to cause long-term disruption to the vital services in question; (4) Impact on citizens' lives; and (5) Guidelines for citizens in the event of a long-term disruption.

The business continuity plan carries out a review based on the results of the risk analysis, and prescribes a recovery plan that corresponds to scenarios in a class of high risk. The recovery plan should include the following: (1) Contact information of the representative in charge of incident response in the event of disruption to vital services and critical activities; (2) Contents of recovery activities; (3) Contact information of the deputy representative in charge of incident response and contents of activities; (4) Resources necessary for recovery activities; (5) Alternative measures if the recovery activities cannot be implemented effectively; (6) Measures to mitigate damage and the implementation procedures of these measures; (7) Guidelines for the provision of information to citizens; (8) Expected time required for the restoration of vital services.

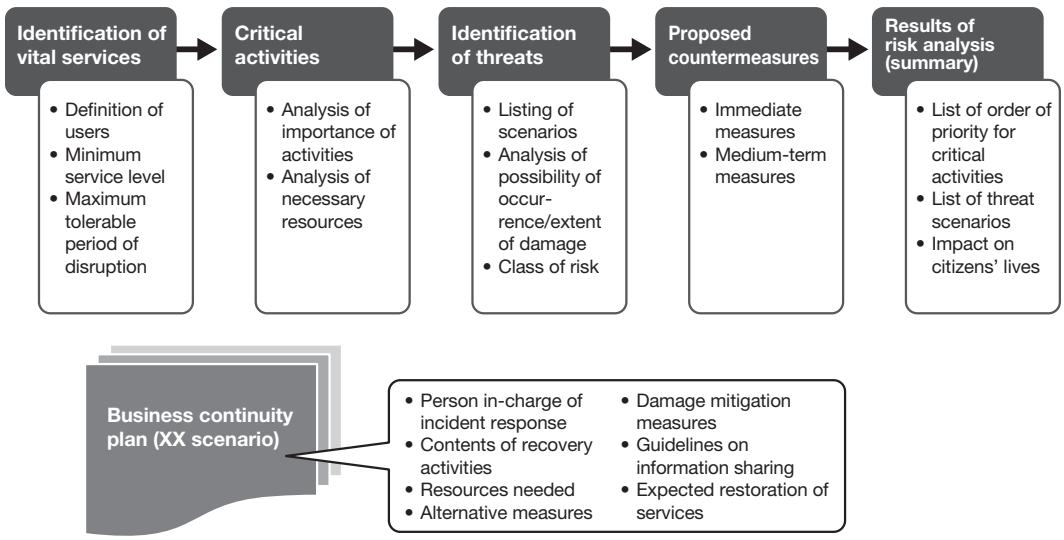


Figure 5 Overview of risk analysis procedures and business continuity plans

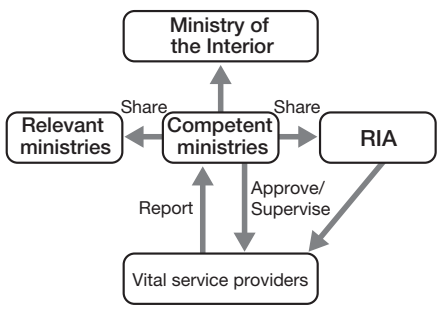
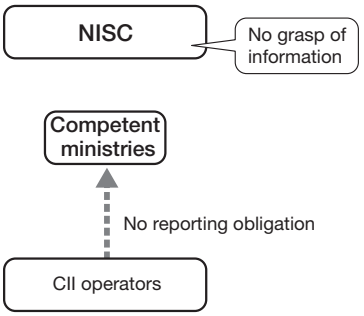
Source: Drawn up based on Estonia's "Requirements and procedure for a continuity risk assessment and plan of a vital service, for the preparation thereof and the implementation of a plan"

(ii) Comparison with Japan's approach to risk analysis and business continuity plans

With regard to the risk analysis and formulation of business continuity plans for critical infrastructure in Japan, Japan implements similar initiatives as Estonia as a part of two policy approaches: the establishment and spread of safety standards, and risk management and establishment of a coping mechanism, which are set forth in the Fourth Action Plan on Information Security Measures for Critical Infrastructures. However, several differences can be found.

In Estonia, it is mandatory to conduct risk analyses and formulate business continuity plans for vital services, with legally binding force provided through the Emergency Act and other relevant domestic laws and ordinances. Under the Estonian system, the risk analyses and business continuity plans drawn up by vital service providers are submitted to the competent ministries and agencies for the vital services, and approved by these competent ministries and agencies. If there are any inadequacies with these risk analyses and business continuity plans, the competent ministries and agencies can provide the necessary supervision. Furthermore, the risk analyses and business continuity plans submitted to the competent ministries and agencies of the vital services are shared not only with the competent ministries and agencies in question, but also with all other relevant ministries and agencies. They are also consolidated at the Ministry of the Interior, which plays a leadership role in responding to emergency situations. Through this framework, the Ministry of the Interior is able to capture the risk analyses and business continuity plans drawn up by all vital service providers, and thereby obtain information beforehand on the response that providers should take if a crisis occurs in relation to vital services. Moreover, as the risk analyses and business continuity plans contain information that is related to the trade secrets of the service provider in question, the protection of these documents is provided for under the Emergency Act. On the other hand, the formulation of risk analyses and business continuity plans in Japan is encouraged as an effort to meet the goals set out in the Fourth Action Plan, but is not legally mandated for CII operators. According to a survey conducted by NISC in FY2016, only 57% of all CII operators have completed the formulation of a business continuity plan, while 23% of the CII

Table 4 Comparison of information-sharing systems of Estonia and Japan

	Estonia	Japan
Legally binding force	Yes Provided for under the Emergency Act	No Fourth Action Plan on Information Security Measures for Critical Infrastructures
Sharing of information with the government		

Source: Drawn up based on Estonia's Emergency Act and the Order for the Organization of the Cabinet Secretariat

operators have no plans to draw up a business continuity plan.[53] This clearly shows the negative effect of a measure that has no legally binding force. Furthermore, risk analyses and business continuity plans are kept internally by the CII operators that have drawn them up; these operators are not obligated to submit them to the competent ministries and agencies of critical infrastructure. For this reason, in Japan, the competent ministries and agencies do not have any means of carrying out supervision or providing instruction with regard to the response of CII operators in the event of a critical infrastructure-related crisis. On top of that, they are also unable to capture the contents of the plans beforehand.

(iii) Feasibility of implementation in Japan

In addition to minimizing the damage caused by cyberattacks, it is possible to enhance resilience with regard to the operation of critical infrastructure by swiftly implementing restoration and recovery procedures. The formulation of a risk analysis and business continuity plan is indispensable toward enhancing the cyber-resilience of critical infrastructure. Although NISC has played a central role in promoting the formulation of risk analysis and business continuity plan among CII operators, but response is progressing slowly.

In order to ensure that CII operators comply with the requirement of drawing up risk analyses and business continuity plans, it is necessary to make it legally mandatory. As explained in the previous section about legal systems, the Basic Act on Cybersecurity should be revised to make CII operators should be obligated to conduct risk analyses and draw up business continuity plans.

(5) Cyber Exercises

(i) Cyber exercises in Estonia

Estonia recognizes cyber exercises as an important means for promoting public-private partnership. Hence, the government takes the lead in organizing cyber exercises that are participated in by both the public and private sectors. It also participates actively in international cyber exercises.

Cyber exercises organized by the Estonian government include “Cyber Hedgehog”, which is based on the scenario of a cyberattack on the electronic voting system, as well as the tactical exercise on the protection of critical infrastructure and crisis management organized by the Ministry of Economic Affairs and Communications, both held in 2010. Cyber Fever, a command center exercise for cyber defense by the Estonian government, was held in 2012, during which the decision-making process in the government was confirmed.

The Cyber Defense Unit (to be discussed later) participates every year in Spring Storm, the military exercise conducted by the Estonian military, during which it participates in training on public-private partnership in emergencies. Since 2013, RIA has been organizing a technical training every year, which draws about 500 to 800 participants from the private sector annually, including vital service providers.

In 2015, the Ministry of Economic Affairs and Communications organized CONEX2015 in cooperation with the Ministry of the Interior. This exercise verified the response guidelines at the strategic level in the event of information leakage incidents and large-scale cyberattack on vital

[53] National center of Incident readiness and Strategy for Cybersecurity (NISC), “FY2016 Survey on the Status of Penetration of Safety Standards, etc. for Critical Infrastructure,” http://www.nisc.go.jp/conference/cs/ciip/dai10/pdf/10shiryou02.pdf.

services such as the eID card infrastructure and data exchange networks. Furthermore, Cyber Hedgehog 2015 held the same year provided validation based on the emergency response plan for large-scale cyberattacks, for matters such as the role of the respective organizations during an emergency, guidelines for public-private partnerships, response procedures in RIA, and guidelines for the sharing of information.

Based on the results of CONEX2015 and Cyber Hedgehog 2015, a review was carried out on the types of vital services covered under the Emergency Act, as well as the revision of regulations in the laws governing each sector. In 2017, the revised Emergency Act was enforced. In this way, cyber exercises conducted in Estonia do not only enhance participants' capacity and verify response procedures; rather, the results of the exercises are swiftly tied in with law revisions in order to ensure that the respective organizations respond securely when coping with an emergency. This is the characteristic of the Estonian system.

With regard to involvement in international cyber exercises, Estonia has participated in Cyber Europe organized by EU/ENISA (2010, 2012), the joint EU-US exercise Cyber Atlantic (2011), Cyber Coalition organized by NATO (2011), NATO's crisis management exercise CMX (2012), and Baltic Cyber Shields (2010) and Locked Shields (2012) organized by the NATO Cooperative Cyber Defence Centre of Excellence, to name a few. The Cyber Defense Unit participated in Cyber Coalition in 2009 as an observer, and has been participating every year since 2010. At Cyber Coalition held in 2012, employees of vital service providers in Estonia also provided their cooperation from the planning phase.[54] At the Locked Shields exercise held in 2013, the Estonian representative team, comprising vital service providers and key members of RIA, was highly appraised for its advanced technical skills and excellent teamwork, and placed second after the NATO representative team.[55] The 2013 Cyber Coalition exercise was hosted by Estonia. In addition to preparing the plans for the exercise through public-private cooperation, cyber experts from the private sector of Estonia led the exercise during its implementation, marking a first for an exercise organized by NATO.[56] From the beginning of 2014, Estonia has been even more actively involved in international cyber exercises. At the Cyber Europe exercise organized by EU, nine teams from Estonia composed jointly of members from the public and private sectors participated and confirmed guidelines for incident response, information-sharing, and inter-agency coordination. In addition, key personnel from RIA were also involved in the preparation of exercise plans, coordination of the exercise, and as key "red team" members. At Cyber Coalition, the Estonian representatives surprised the other participating countries by demonstrating their advanced skills in carrying out digital forensic investigation on android terminals that have been contaminated by malware. At Locked Shields, the Estonian team was ranked third overall, and first in the forensics category.[57] The Locked Shields exercise held in 2017 was hosted by Estonia, and was conducted based on the scenario of defending a virtual airbase network from cyberattacks on power networks, reconnaissance drones, the military's command and control system as well as fuel

---

54 Piret Pernik and Emmet Tuohy, *Interagency Cooperation on Cyber Security: The Estonian Model*, p. 9.

55 Republic of Estonia Information System Authority, *2013 Annual Report Cyber Security Branch of the Estonian Information System Authority,* p. 14.

56 Piret, *Interagency Cooperation on Cyber Security: The Estonian Model*, p. 9.

57 Republic of Estonia Information System Authority, *2014 Annual Report Cyber Security Branch of the Estonian Information System Authority*, p. 21.

supply infrastructure.

To date, Locked Shields had been an exercise focused primarily on the technical aspects. However, in the Locked Shields exercise hosted by Estonia, training was also conducted on decision-making processes for policymakers, with support provided by legal advisors. All the exercises are participated in by government organizations, Internet service providers, and practitioners from vital service providers, who present a high level of skills. These international cyber exercises are characterized by the active involvement of not only key government officials from Estonia, but also engineers from the private sector.

(ii) Comparison with Japan's approach to cyber exercises

In Japan, cross-sectoral exercises organized by the Cabinet Office have been held since FY2006 with the aim of improving public-private partnership in the field of critical infrastructure protection. The exercise scenarios have been becoming increasingly difficult, while the scale of the exercise has also been expanding, from about 90 participants in FY2006 to about 2,600 participants in FY2017. Each competent ministry and agency of critical infrastructure has also been conducting exercises on dealing with cyberattacks, with a focus on their respective areas of jurisdiction.

Although similar cyber exercises are also conducted in Estonia, the difference with Japan lies in the fact that Estonia's exercises provide training on the response by various governmental organizations to large-scale cyberattacks, and validate the effectiveness of the country's emergency response plans. Japan's cross-sectoral exercises, on the other hand, are focused on the sharing of information and collaboration between the critical infrastructure stakeholders, while exercises conducted by the competent ministries and agencies of critical infrastructure are aimed at enhancing the technical response capability of operators in their respective fields. Going forward, the respective ministries and agencies of the Japanese government should actively incorporate training that includes aspects such as response and decision-making, into their exercises.

It has to be said that Japan's involvement in international cyber exercises is relatively limited in comparison with Estonia. In the past, Japan had participated in Cyber Storm, a public-private joint exercise organized by the US Department of Homeland Security.[58] The government and CII operators have a poor track record for full-fledged participation in international cyber exercises. In September 2017, the Ministry of Economy, Trade and Industry held the first US-Japan ICS (Industrial Control System) Cybersecurity Joint Training in Japan.[59] Seven experts from the US Department of Homeland Security and ICS-CERT were invited, and an exercise on cybersecurity for industrial control systems was finally held. Estonia has attracted the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) into its country, and makes use of its geographical advantage to participate as a player in various international cyber exercises organized by NATO and EU. It is also involved in the preparation of exercise plans, prior coordination, leading the exercises, and as the "red team" (playing the role of the attackers). In addition to employees of governmental organizations, engineers of vital service providers also participate actively. In these respects, it differs greatly from Japan.

---

[58] Cabinet Secretariat, *"Jyoho Sekyuriti Seisaku no Gaiyo"* [Overview of Information Security Policy], p. 12. http://www.kantei.go.jp/jp/singi/shin-ampobouei2010/dai7/siryou2.pdf.

[59] Ministry of Economy, Trade and Industry, "Press Release: Japan's first US-Japan ICS (Industrial Control System) Cybersecurity Joint Training held," http://www.meti.go.jp/press/2017/09/20170927004/20170927004.html

Table 6 Comparison of Estonia and Japan in the area of cyber exercises

	Estonia	Japan
Domestic cyber exercises	• Government's decision-making exercise (CONEX) • Public-private cooperation exercise (Cyber Hedgehog) ⇒ Confirmation of request for emergency response, revision of law	• Cross-sectoral exercises ⇒ Confirmation of public-private cooperation guidelines
International cyber exercises	• Proactive involvement in cyber exercises organized by EU and NATO • Planning and leading of exercises as a host country • Self-directed involvement by the private sector, such as vital service providers, Internet service providers, etc.	• Participation in Cyber Storm (U.S.), etc. as observer • Organized US-Japan ICS Cybersecurity Joint Training (METI) (September 2017), seven participants from U.S.

Source: Drawn up based on the status of participation in cyber exercises by Estonia and Japan

(iii) Feasibility of implementation in Japan

In Estonia, cyber exercises are carried out based on the assumption of a large-scale cyberattack on vital services, and various matters are verified based on the emergency response plan, including the government's decision-making processes, the roles of the respective organizations in an emergency, guidelines for public-private cooperation, response procedures in RIA, and guidelines for information-sharing. In Japan as well, efforts are made to build the response capacity of vital service providers through cross-sectoral exercises. By making use of the framework of such cross-sectoral exercises, which are conducted based on the scenario of a large-scale cyberattack at the national level as explained in the previous section, it is possible to verify the emergency response plans drawn up by the government, the guidelines for strategic decision-making by policymakers, response by the respective ministries and agencies, and public-private partnership.

Involvement in international cyber exercises, which is actively promoted in Estonia, can also be fully introduced in Japan. Through the active participation of engineers from government organizations, CII operators, and cybersecurity operators in international cyber exercises held in Europe and America, Japan can acquire information about the latest cyberattack technology and defense technology, as well as develop friendly relations and human networks with the relevant countries. Furthermore, acquiring knowhow on organizing international cyber exercises can also facilitate the hosting of international cyber exercises by Japan in future.

(6) National Defense Strategy and Organizations

(a) Positioning of cyber defense and protection of vital services in the national defense strategy

(i) Estonia's national defense strategy and protection of vital services

Estonia is a small country with a small population. Its terrain is flat with few topographical barriers, and shares a border Russia, a potential adversary country. Hence, from the perspective of national defense, it has been placed in a very tough environment. For this reason, its national defense strategy is set out based on the premise of primarily confronting threats from Russia. The National Defense Strategy of Estonia published by the Estonian Ministry of Defense, sets out the decline of Estonia's international status through non-military means and the threat of the severance of friendly relations with allies as security risks faced by Estonia, and raises attacks on

energy-related infrastructure and information and communications systems as a potential threat to Estonia's survival.[60] It establishes "the Estonian population's strong will to defend their country" as the basis of Estonia's national defense, and emphasizes the principle of "total defense" as a means of countering the threat of war as well as non-military threats.[61] The National Defense Strategy sets out six main courses of action to ensure deterrence power as well as organized response for its national defense. These are: military defense; civil sector support to military defense; international efforts; ensuring internal security; ensuring the sustainability of vital services; psychological defense.

Of these six courses of action for its National Defense Strategy, the inclusion of "ensuring the sustainability of vital services" is a distinctive feature, and is consistent with the previously mentioned Cyber Security Strategy 2014 – 2017 and provisions of the Emergency Act. The National Defense Strategy sets out the guidelines for ensuring the sustainability of vital services in the event of a military attack. According to the Strategy, in the event of a military attack against Estonia, sustainability of vital services shall be continued within the same organizational frameworks as would be applied under peacetime circumstances. It then lists the competent ministries and agencies that govern the respective vital services. The Strategy also stipulates that the Estonian government identify the vital services that particular importance should be placed on from the perspective of national defense, that vital service providers take into consideration plans for responding to "military threat scenarios" when drawing up risk analyses and business continuity plans, and that the Ministry of the Interior consolidate these plans into an integrated document and submit it to the Riigikogu (parliament) of Estonia once every four years.

(ii) Comparison with Japan

With regard to the security environment surrounding Japan, the National Defense Program Guidelines for FY2014 and Beyond states that establishing the stable use of cyberspace as global commons is a significant security challenge for the international community, including Japan.[62] However, concerning public-private partnership in the field of cyberspace and the protection of critical infrastructure, these Guidelines stop short at stating that "in light of society's growing dependence on outer space and cyberspace, Japan will make effective use of the SDF's capabilities when endeavoring to strengthen collaboration with relevant organizations and clarify the division of roles, thereby contributing to comprehensive, government-wide initiatives."[63] It does not contain any particular reference to the protection of critical infrastructure in relation to cyber security. However, a document titled "Toward Stable and Effective Use of Cyberspace" published by the Ministry of Defense in 2012 states, under the section on "Contributions to National Efforts, including Partnership with the Private Sector," that as the Ministry of Defense and Self-Defense Forces rely on the private sector for the development and maintenance of social infrastructure and equipment, it is important to ensure the stable use of cyberspace across the whole of society. To that end, it states that Japan is engaged in efforts such as conducting cyber exercises, sharing

60 Estonian Ministry of Defence, "National Defence Strategy Estonia", 2011, p. 7.

61 Ibid., p. 8.

62 *National Defense Program Guidelines for FY2014 and Beyond*, approved by the Cabinet (December 17, 2013), p. 2.

63 Ibid., p. 13.

information, and dispatching human resources to government organizations.[64]

In comparing the defense strategies of Estonia and Japan, both countries demonstrate a similar recognition of the importance of cyber defense and the need for public-private partnership. However, while Estonia positions the protection of vital services as one of six courses of action in its national defense, Japan's Ministry of Defense and Self-Defense Forces adopt the position of contributing to government-wide initiatives. Hence, there appears to be a difference in the level of commitment to protecting critical infrastructure between the two countries.

(iii) Feasibility of implementation in Japan

The protection of vital services is positioned as one of the courses of action in the national defense strategy of Estonia, while Japan's Ministry of Defense and Self-Defense Forces adopt only a stance of contributing to comprehensive initiatives by the government as a whole without clearly establishing the functions of the Ministry of Defense and Self-Defense Forces in protecting critical infrastructure. If the protection of critical infrastructure were positioned as a new function of the Ministry of Defense and Self-Defense Forces as a part of Japan's national defense strategy, there would be a need to clarify the scope of their duties, and to enhance the personnel and equipment needed for them to perform these duties.

(b) National defense organizations

(i) Overview of the Estonian Defense Forces

The Estonian Defense Forces are composed of the regular land, sea, and air forces, as well as the Estonian Defense League (hereafter, "Defense League"). The strength of the regular military force during peace time is about 6,000 personnel, half of whom are personnel drafted in under the conscription system. The Defense League is a volunteer national defense organization that comprises about 15,000 personnel. During war time, it is expanded to a 60,000-strong force through the mobilization of reserve personnel who have completed their training under the conscription system.[65]

(ii) Cyber Command of the Estonian Defense Forces

The organization for cyber defense in the Estonian Defense Forces had comprised only personnel from the regular forces deployed to the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE), and the Cyber Defense Unit of the Estonian Defense League (to be discussed later). However, on August 1, 2018, the Cyber Command was newly established as a subordinate organization under the Estonian Land Forces.

The main mission of the Cyber Command is to "carry out operations in cyberspace in order to provide command support for Ministry of Defense's area of responsibility," and its primary tasks are outlined as follows:

- Provide information and communication technology infrastructure and services.
- Provide cyber defense.
- Plan and execute cyber operations.

---

64 Ministry of Defense, *Toward Stable and Effective Use of Cyberspace*," pp. 8-9.

65 Estonian Defence Forces, http://www.mil.ee/en/defence-forces.

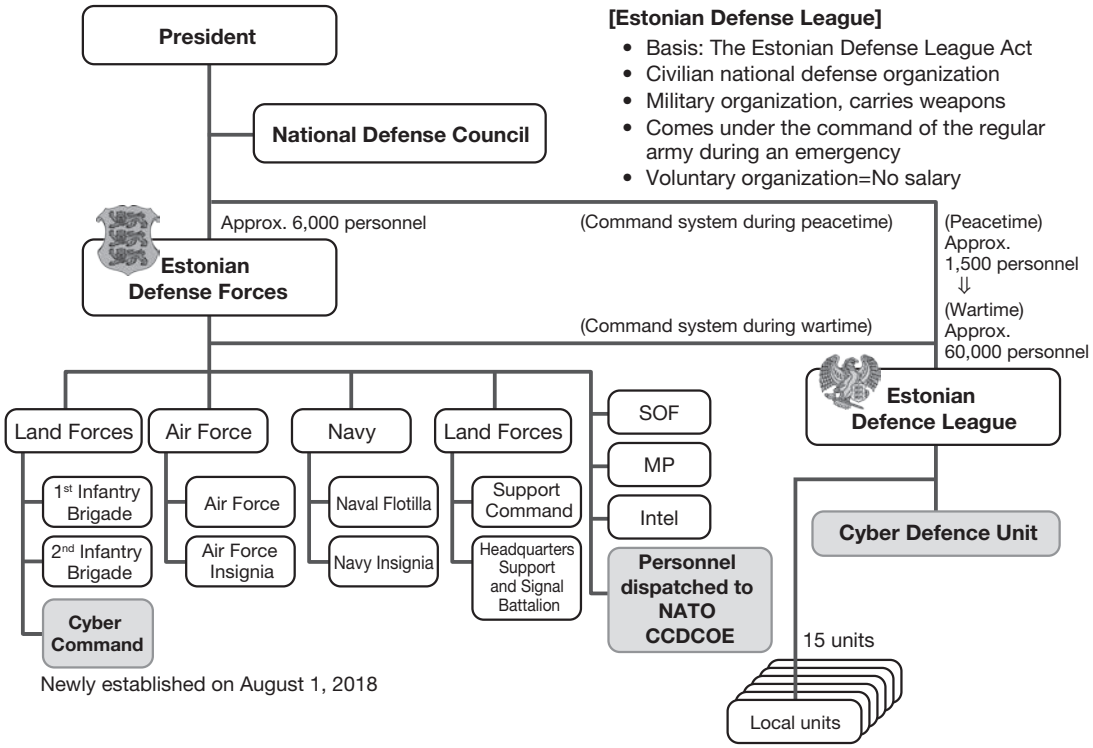


Figure 6 Overview of the organization of the Estonian Defense Forces

Note: The Cyber Command was newly established as a subordinate unit of the Land Forces on August 1, 2018.
Source: Drawn up based on the website of Estonian Ministry of Defense

- Gain, maintain and share cyberspace situation awareness.
- Plan and execute information operations.
- Provide Headquarters support for Joint Headquarters.
- Plan and execute strategic communications.
- Train, prepare and mobilize wartime and reserve units.
- Conduct functional area Training, Research and Development.

The Cyber Command of the Estonian Land Forces is organized as follows: Headquarters, HQ Support and Signal Battalion, Information Communication Technology Center, Cyber and Information Operations Center, Strategic Communications Center, and HQ and Support Company.[66] It has a strength of about 300 personnel (about 240 personnel from the existing communications unit, and about 60 newly recruited personnel), and its combat capability is expected to be completed by 2023.[67]

66 Cyber Command, http://www.mil.ee/en/landforces/Cyber-Command.

67 Kaitsevae kubervaejuhatus alustas tegevust (The Cyber Command of the Defense Forces began its attivities), http://www.mil.ee/et/uudised/10340/kaitsevae-kubervaejuhatus-alustas-tegevust.

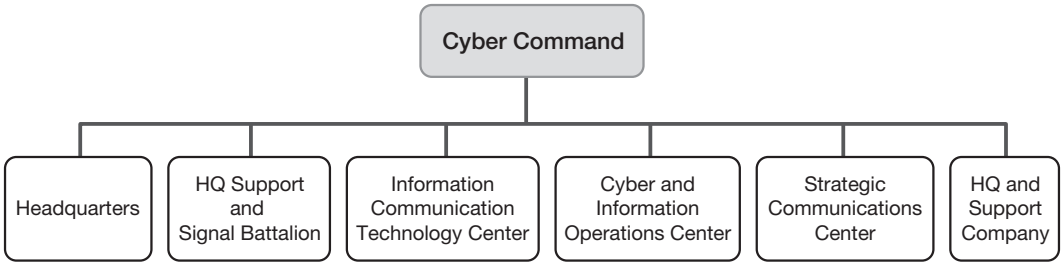


Figure 7 Organization of the Cyber Command of the Estonian Land Forces

Source: Extracted from the website of the Estonian Defense Forces

(iii) Cyber Defense Unit of the Estonian Defense League

To understand the cyber defense system of the Estonian Defense Forces, it is first necessary to gain an overview of the Estonian Defense League, which is a paramilitary organization.

The Estonian Defense League is defined as a civilian national defense organization under the Estonian Defense League Act (hereafter, "Defense League Act"), which provides for its organization as a military organization, its possession of arms, implementation of training, and incorporation under the command of the regular army in the event of an emergency. Civilians participate in the Defense League through their own free will, and they are not paid any salary as the Defense League is a voluntary organization.[68]

The Commander of the Defense League is appointed by the Estonian government based on recommendations put forth by the Minister of Defense and the Commander of the Defense Forces. Within the command system, the Commander of the Defense League is subordinate to the Commander of the Defense Forces. However, during peace time, the authority of the Commander of the Defense Forces to direct the Defense League is limited only to matters related to military training, while authority over the management and operation of the Defense League is exclusive to the Commander of the Defense League. During an emergency, the Commander of the Defense Forces has full command over the Defense League.

The Cyber Defense Unit is a unit that is in parallel with the 15 regional units under the Defense League, and comprises the Unit Commander, Unit Command, and multiple cells. The Unit Command is a staff organization that supports the decision-making of the Unit Commander, and the respective departments including logistics and supplies, analysis, and training, are made up of both volunteers and full-time personnel. There are multiple cells within the Unit that are engaged in various missions related to cyber defense, as well as maintenance and management, research, and tool development, among others.[69]

(iv) Mission of the Cyber Defense Unit

The core tasks of the Cyber Defense Unit are to provide education and training, and strengthen cybersecurity in the private sector.

Education and training, which is the first core task of the Cyber Defense Unit during

[68] Kadri Lasla, Anna-Maria Osula, LTC Jan Stinissen, *The Cyber Defence Unit of the Estonian Defence League*, p. 10.

[69] Ibid., pp. 13-14.

peacetime, aims to enhance the knowledge, skills, experience, and attitude in executing missions of key personnel. Seminars, information sharing study sessions, training, and field studies are planned for personnel. They also participate in the Locked Shield exercise and the Spring Storm exercise organized by the Estonian Defense Forces, improve their cyber defense skills, and master incident coping skills and information sharing procedures during emergencies.

The second core task of the Cyber Defense Unit is to strengthen cybersecurity in the private sector. In this respect, a wide range of technical support is provided to various public and private organizations to contribute to the strengthening of cybersecurity. Some examples of the initiatives implemented in this regard include consulting on security measures, implementation of tests on the security functions of information systems, malware screening on the computers of municipal schools, installation of security functions for the national electronic voting system, and security examinations.

Other tasks include providing support for cybersecurity for information and communication systems, and ensuring cybersecurity in times of emergency.

In particular, the Emergency Act sets out provisions for the Defense League to respond in the event of an emergency in order to limit the extent of damage, while the Cyber Defense Unit responds during a cybersecurity-related emergency, such as a large-scale cyberattack on critical services. Although the specific duties are not clearly stipulated, the government assigns the responsibilities on a case-by-case basis during such situations.[70]

(v) Recruitment of personnel, and their obligations and responsibilities

To be accepted as a member of the Cyber Defense Unit, personnel is required to be 18 years or older, have an impeccable personal and career history, be loyal to Estonia, and be strongly committed to protecting Estonia's independence and complying with the constitution. Not all personnel recruited are cybersecurity experts or individuals with advanced IT skills; lawyers, policymakers, and educators in the field of cybersecurity, among others, are also hired.[71] Candidates need to receive recommendation letters from two personnel who have already been hired by the Cyber Defense Unit, and these two recommending personnel are responsible for the candidate's suitability for the job. Those who are known to have health issues, criminal records, or observed to demonstrate inappropriate behavior, are not accepted. Candidates submit application forms to the Commander of the Cyber Defense Unit, undergo a background check, and a decision is made on whether the candidate is accepted or rejected within approximately three months. If accepted, the candidate is sworn in and officially joins the Unit.[72]

Personnel are required to protect Estonia's independence as well as constitutional order, and to comply with laws and regulations in carrying out the activities of the Defense League. Being a member of the Cyber Defense Unit in itself does not make it compulsory for personnel to participate in the activities of the Defense League. To begin with, the Defense League is an organization established through participation base on the free will of members. As such, whether or not to partake in a specific mission rests on the free will of the respective personnel. In particular,

---

70 Ibid., pp. 22-24.

71 Estonian Defence League's Cyber Unit, http://www.kaitseliit.ee/en/cyber-unit.

72 Kadri, *The Cyber Defence Unit of the Estonian Defence League*, pp. 15-17.

personnel of the Cyber Defense Unit participate in activities as volunteers without receiving any remuneration from the government, while receiving a salary through their day jobs in regular companies. As such, they participate in the activities of the Cyber Defense Unit in spare moments between their main jobs. When carrying out a mission, they are required to wear either the uniform of the Defense League, or to wear the badge of the Defense League on their own attire.[73]

(vi) Logistical support and access to confidential information

The Cyber Defense Unit is allocated with the necessary equipment for performing its duties in coordination with the Estonian Defense Forces and the Ministry of Defense. The Defense League has the right to use the facilities and equipment of the Estonian Defense Forces for free, through prior arrangements and coordination. The information and communications infrastructure managed by the Cyber Defense Unit is supplied through contracts with external parties. The expenses related to the operation of the Cyber Defense Unit are covered by the government's budget, as well as subscriptions, donations, and revenue from contracts.[74]

In performing its duties, the Cyber Defense Unit needs to access the information of public and private vital service providers, and for both the public and private sectors, the detailed information concerning critical infrastructure often constitutes confidential information that cannot be disclosed. Access to information on critical infrastructure in the private sector is managed through the conclusion of non-disclosure agreements concerning the handling of information for support missions during peacetime. However, in an emergency, there is no choice but to respond on a case-by-case basis. This is viewed as an issue that should be resolved going forward.

As for the critical infrastructure operated and managed by the national government, the smallest number of volunteers needed for the Cyber Defense Unit is subjected to security screening, and a system has been established that enables them to access confidential information on an official basis. The types of confidential information that can be accessed by these personnel are determined in accordance with the principle of "need to know," based on the judgement of the manager of the critical infrastructure. Hence, assigning security clearance to the personnel of the Cyber Defense Unit ensures that they do not pose a risk to information security.[75]

(vii) Status under international law in the event of an international armed conflict

The respective units of the Defense League, including the Cyber Defense Unit, carry out their respective missions under the leadership of the Commander of the Estonian Defense Forces in the event of an international armed conflict. As the personnel of the Defense League are organized through the participation of private-sector volunteers, measures are taken to ensure that they fulfill the qualifications of combatants in accordance with international law.

Under international law, members of an army fall into two categories. The first category comprises members of the regular army of the countries involved in the conflict, and includes militia or volunteers who make up a part of the regular army. The second category comprises members of the militia or volunteers other than the aforementioned, and includes organized

---

73 Ibid., pp. 18-19.
74 Ibid., p. 27.
75 Ibid., pp. 31-32.

resistance activities that belong to the countries involved in the conflict. Such organizations are deemed as members of the army by fulfilling the following four criteria set out in the international customary law and Article 4A(2) of Geneva Convention (III).

(1) Under the command of a single person who is responsible for his/her subordinates.
(2) Wearing a fixed unique badge that can be identified from a certain distance away.
(3) Carries weapons openly in the public.
(4) Carries out operations in accordance with the law of armed conflict and customary law.

An irregular unit that belongs to countries involved in the conflict, and which fulfill the four criteria set out above, is qualified to be a combatant unit, and is exempted from combatant liability while having prisoner-of-war status.[76]

Let us attempt to apply the provisions of these international laws to the Defense League.

Firstly, as the Defense League comes under the command of the Estonian Defense Forces during wartime, members of the Cyber Defense Unit correspond to the first category of militia or volunteers who form a part of the regular army. On the other hand, the Defense League during peacetime does not fall under the command of the Estonian Defense Forces. For this reason, it does not correspond to the first category of militia or volunteers who form a part of the regular army, but corresponds to the second category of other militia or volunteers and therefore is required to fulfill the four criteria. With regard to the four criteria to be deemed as a member of the army, the first criteria require it to be under the command of a single person who is responsible for his/her subordinates. The Defense League clearly fulfills this, with a Commander of the Defense League and a Unit Commander of the Cyber Defense Unit, which is a subordinate unit under the Defense League. As for the second criteria of wearing a fixed unique badge that can be identified from a certain distance away, members are required to wear the uniform or wear the badge of the Defense League over their own attire, so this condition is also fulfilled. The third criteria of carrying weapons openly in publics is not particularly meaningful in the context of cyberwarfare. With regard to the fourth criteria of carrying out operations in accordance with the law of armed conflict and customary law, education and training on the law of armed conflict are implemented regularly, while operations are carried out in accordance with international law under the command of the Unit Commander in times of emergency. Hence, this criteria is also fulfilled.

Based on the above, regardless of any declaration of war or whether or not there is a clear armed attack, civilian volunteers who are the members of the Cyber Defense Unit are qualified as combatants under international law, and can perform various duties as members of the Estonian Defense Forces.[77]

(viii) Comparison with Japan

In the case of Japan, the Cyber Defense group is made up of the SDF Command Control Communication Computers Systems Command and the respective communications and system defense groups of the land, maritime, and air defense forces. Personnel of the respective cyber defense units comprise only members who have been nurtured through education and training

[76] Michael N. Schmitt, *TALLIN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS Second Edition*, Cambridge University Press, p. 403.

[77] Kadri Lasla, Anna-Maria Osula, LTC Jan Stinissen, *The Cyber Defence Unit of the Estonian Defence League*, pp. 34-36.

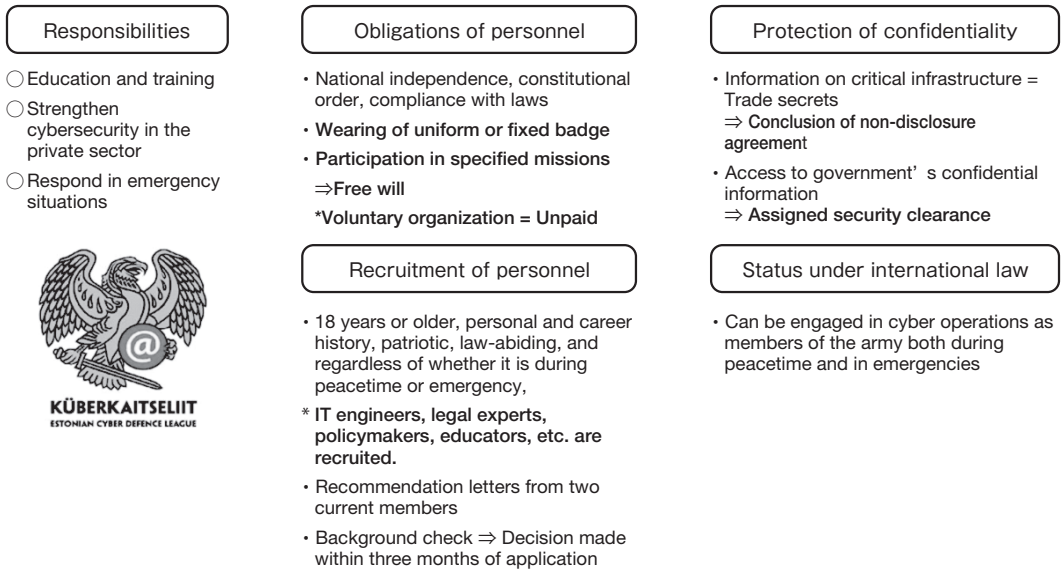


Figure 8 Overview of Cyber Defense Unit

Source: Drawn up based on the reference literature (*The Cyber Defence Unit of the Estonian Defence League*)

within the Self-Defense Force. In Estonia, the cyber defense system is constituted primarily of the Cyber Defense Unit of the Estonian Defense League, which is a paramilitary organization made up of civilian volunteers. However, in August 2018, a new Cyber Command was established under the Estonian Land Forces, which is the regular army of Estonia.

Comparing Japan and Estonia from the perspective of national defense organizations related to cyber defense, a significant difference is observed. In Japan, although SDF reserve personnel system that utilizes civilians has been put in place, it does not specialize in cyber defense. On the other hand, in Estonia, the cyber defense force is composed primarily of the Cyber Defense Unit, a paramilitary organization made up of civilians. (Alongside with the establishment of the new Cyber Command, which is a regular military unit, there is a need to pay attention to the command systems and relationship between the regular military unit of the Cyber Command and the paramilitary organization of the Cyber Defense Unit in future.)

Members of the Cyber Defense Unit are engaged in their day jobs (such as in IT corporations in the private sector or as university professors), while at the same time build up their own capacity through various training programs designed by the Cyber Defense Unit. In times of emergency, they participate in the defense of the country's critical infrastructure. Through the activities of the Cyber Defense Unit, cybersecurity personnel from government organizations and a wide range of industrial sectors interact and engage in exchanges from peacetime, making it easier to cooperate when an incident occurs. Smooth response can therefore be expected.

There is a shortage of experts in the field of cybersecurity not only in Japan but in countries around the world. Although government organizations and corporations are frantically engaged in the competition for human resources with advanced capabilities, Estonia's initiatives are characterized not by the capturing of human resources with advanced capabilities, but in the use of the method of providing a space for national defense activities in cyberspace.

Table 7 Comparison of the national defense strategies and organizations of Estonia and Japan

	Estonia	Japan
National defense strategy	• Positioning of the maintenance of vital services as a main course of action in the national defense strategy	• No particular points raised about the defense of critical infrastructure (Contributing to government-wide initiatives including the private sector)
National defense organization (cyber)	• Main entity: Cyber Defense Unit of the Defense League * After August 2018, the newly established Cyber Command is expected to become the main entity • Main responsibilities: Education and training, strengthening of cybersecurity in the private sector, response during an emergency	• Main entity: Cyber Defense Group, etc. * Means of utilizing civilians not yet developed • Main responsibilities: Defense of SDF's system and network

Source: Drawn up based on Estonia's National Defense Strategy and other documents, and the Defense of Japan

(ix) Feasibility of implementation in Japan

While a Cyber Defense Unit that utilizes civilian volunteers is an extremely beneficial and appealing system, if a similar system were to be introduced in Japan, it is still unknown if the system will be accepted, and whether it can become an established institution. For example, Marine Rescue Japan is an example of a voluntary organization in the area of maritime security. Marine Rescue Japan is a public rescue system supported by national and local government agencies such as the Japan Coast Guard, police, and fire department. As such, it assists in the activities of civilian voluntary rescuers participating in the rescue of people or boats in distress in coastal waters. In addition, the fire corps system under the fire department, while not a voluntary organization, can also serve as a reference. Unlike full-time firefighters, members of the fire corps have other jobs but are mobilized during disasters and for training. They are engaged in keeping guard against fires, putting down riots, disaster prevention, mitigation of damage, as well as support and awareness-raising activities for local residents.

Hence, volunteer activities that support public organizations and systems such as a fire corps can possibly be applied to the field of cybersecurity. However, in the case where such volunteer organizations are associated with the activities of the Ministry of Defense and Self-Defense Forces, which are responsible for national defense, it is necessary to resolve the problems related to the status of personnel under international law. In an international armed conflict, when general civilians are involved in various actions carried out by the Ministry of Defense and Self-Defense forces in relation to cyber defense, there is a possibility that this may correspond with direct participation in hostility by civilians through connection with the three cumulative standards: the threshold of harm, direct causality, and combatants. This may in turn be deemed as committing a (war) crime. To resolve this issue, Estonia's Cyber Defense Unit has designed its system cautiously to ensure that the civilian volunteers are recognize as combatants under international law, in preparation for the event that a large-scale cyberattack is carried out as a part of an international armed conflict.

If Japan were to introduce the effective aspects of Estonia's Cyber Defense Unit system, it would be appropriate to first promote the establishment of a voluntary organization under the

leadership of the government, utilize the existing SDF reserve personnel system, and build a system that allows cybersecurity experts from the private sector to be involved in national defense.

4. Policy recommendations for promoting public-private partnership

Up till this point, this paper has conducted an overview of public-private partnership initiatives related to Japan's cyber defense. It then looked at the various policies of Estonia, undertook a comparison with Japan, and considered the feasibility of implementing these cybersecurity policies in Japan. Based on these reviews, this section offers several policy recommendations for promoting public-private partnership for Japan's cyber defense.

(1) Review of the cybersecurity strategy

Japan's cybersecurity strategy should position cybersecurity for critical infrastructure as the issue of top priority. With regard to the respective policy approaches set out in the cybersecurity strategy, it should clearly set out the order of priority based on an analysis of the respective degree of importance and level of urgency.

Japan's current cybersecurity strategy sets out the following four policy approaches: Enabling socio-economic vitality and sustainable development; Building a safe and secure society for the people; Contribution to the peace and stability of the international community and Japan's national security; Cross-cutting approaches to cybersecurity. The first policy approach, "Enabling socio-economic vitality and sustainable development," can only be realized by ensuring the security of Japan and the stable functioning of critical infrastructure that is the basis of our socio-economic system. The suspension of the functions of critical infrastructure through a large-scale cyberattack can cause damage that has a severe impact on citizens' lives and socio-economic activities, and is also a highly probable event. It is clear that ensuring cybersecurity for critical infrastructure is a matter of the highest priority in comparison with other measures.

From this perspective, Japan's cybersecurity strategy should clarify the order of priority of measures as well as the priority matters, rather than simply listing the policy approaches. At the same time, it should position measures for the protection of critical infrastructure as an issue of the highest priority. Furthermore, alongside with strengthening information-sharing systems between the public and private sectors in order to enhance attribution ability for identifying the masterminds behind attacks, the explicit declaration of putting in place various measures for enhancing the overall resilience of critical infrastructure can also be expected to have considerable effect of deterring the attackers.

(2) Strengthening the supervision and guidance of critical information infrastructure (CII) operators

If we were to consider the probability of a large-scale cyberattack on critical infrastructure and the degree of severity of damage, carrying out a risk analysis and the formulation of a business continuity plan are the responsibilities of CII operators, and the implementation of these activities should be supervised and guided by the government.

However, the current Basic Act on Cybersecurity only calls for CII operators to engage in cooperative efforts for the cybersecurity measures implemented by the government and local public organizations; there is no legal obligation for them to engage in such cooperation. For this reason, in addition to the fact that CII operators are lagging behind in conducting such risk

analyses and formulating business continuity plans, the government has no means of capturing the contents of these plans.

To resolve this issue, under the Basic Act on Cybersecurity, set out provisions on the responsibilities of CII operators, which is to conduct risk analyses on cyberattacks on critical infrastructure, draw up and review business continuity plans based on the results of these risk analyses, and report to the Prime Minister via NISC. The Basic Act on Cybersecurity should also set out provisions for the responsibilities of the national government, which is to exert all efforts to secure trade secrets in the results of the risk analyses and business continuity plans submitted by CII operators, draw up emergency response plans for large-scale cyberattacks, and validate and review these plans through exercises and other means. When revising the law, the Basic Act on Disaster Management (Act No. 223 of 1961) can be used as a reference. Article 39 of the Basic Act on Disaster Management states that a designated public corporation must formulate a disaster management operation plan based on the government's basic disaster management plan, review it every year, and report it to the Prime Minister through the competent Minister. By taking this example as a reference and incorporating new provisions in the Basic Act on Cybersecurity, it is possible to mandate CII operators to report to the government on the formulation of business continuity plans.

The revision of this law can eliminate delays by CII operators to conduct risk analyses and formulate business continuity plans. At the same time, based on the risk analyses and business continuity plans reported by the CII operators, the government can draw up a cross-agency emergency response plan for a large-scale cyberattack at the national level.

(3) Enhancing the functions of the National center of Incident readiness and Strategy for Cybersecurity (NISC)

Ensuring cybersecurity for critical infrastructure in Japan is based on the voluntary efforts of CII operators. The competent ministries and agencies of the respective fields of critical infrastructure have the authority to supervise CII operators, which is based on laws governing the respective industries. Under the current system, the Cybersecurity Strategy Headquarters and NISC do not have direct supervision authority over CII operators. For this reason, measures are promoted through advice and recommendations, as well as general coordination with the competent ministries and agencies of critical infrastructure. As the implementation of cybersecurity policies for critical infrastructure is under the jurisdiction of the respective competent ministries and agencies, there is a possibility that differences may arise in the security measures for each field of critical infrastructure. Moreover, it is not efficient as there is a need to assign a supervising manager and establish a supervising department for cybersecurity in each competent ministry and agency.

For this reason, as demonstrated by the example of RIA in Estonia, a system that enables the unified implementation of security measures for all critical infrastructure should be established by concentrating the supervisory authority for the execution of cybersecurity policies by CII operators on NISC. In doing so, the cybersecurity-related departments of IPA and NICT, as the executive organs for the supervisory work, should be utilized in projects commissioned by the government to establish a system for enabling the implementation of supervisory work on CII operators.

(4) Preparing for a large-scale cyberattack at the national level as a form of armed attack

In promoting public-private partnership in cyber defense, exercises implemented jointly by the public and private sectors is an extremely effective means. In the event of damage to critical infrastructure due to a large-scale cyberattack, response should not be made only by the CII operator that has incurred damage; rather, there is a need for the competent ministries and agencies of the critical infrastructure in question, emergency response organizations such as CERT, and other CII operators to work as one to respond. To enable joint response by the respective public and private-sector actors, it is important to prepare the procedures for dealing and responding to incidents, and to validate their effectiveness.

In particular, with regard to large-scale cyberattacks on critical infrastructure, there is a strong likelihood of a situation that requires a judgement call on whether or not an attack has been carried out on Japan as a form of armed attack. In the Locked Shields exercise organized by NATO, in parallel with a technical offense and defense exercise based on the scenario of a cyberattack on critical infrastructure and air base, a strategic decision-making exercise by policymakers was also held. To ensure that Japan is able to respond appropriate in such situations, cyber exercises based on the scenario of a large-scale cyberattack on critical infrastructure, launched as a part of an armed attack, should be implemented, and the recognition of the situation, responses by the Ministry of Defense and Self-Defense Forces, as well as response by CII operators should be validated.

(5) Establishing pro-bono cyber defense organizations, and enhancing and utilizing the SDF reserve personnel system

To utilize the limited number of cybersecurity experts effectively, it is effective to build a mechanism similar to the Cyber Defense Unit of Estonia, through which civilians can participate in the cyber defense of the country as a social contribution activity. To track the approximately 58 billion yen worth of virtual currency that had leaked out from a virtual currency exchange company in January 2018, dozens of engineers acting in good faith ("white hackers") participated in the effort.[78] In cases such as this, we can see how civilians with advanced cybersecurity skills can help in dealing with cyber incidents as a goodwill activity. In the large-scale cyberattack that occurred in Estonia in April 2007, cybersecurity engineers from within and outside Estonia supported CERT-EE through an ad-hoc and informal human network. The success of Estonia's Cyber Defense Unit system can probably be attributed to the provision of a space where such good-intentioned engineers can participate in the noble activity of supporting the "cyber defense of the motherland." In addition to employees of government agencies, information and communications corporations, and the information security departments of general corporations, white hackers are present in various sectors. It would be effective for the government to provide a space for highly-skilled white hackers to play an active role in.

The first policy for realizing these goals is support for the establishment of pro-bono cyber defense organizations. In recent years, in addition to general volunteer activities, "pro-bono activities" (derived from the Latin expression "pro bono publico" meaning "for the public interest") as a form of social contribution have been developing gradually. Working adults

78 Nihon Keizai Shimbun, "NEM Ou Zenryo Hakka, Ryushutsu Jyokyo no Kaisetsu Saito mo" [Goodwill Hackers in Pursuit of NEM Also Set Up Websites Covering the Leakage Situation], https://www.nikkei.com/article/DGXMZO27182300210220 18CC0000/.

participate in these activities by making use of their specialized knowledge and skills. Already, the National Police Agency has drawn up a manual (model)[79] for volunteer activities in the field of cybercrimes, aimed at countering and clarifying the illegal and harmful information circulating on websites and bulletin boards on the Internet, and is promoting activities such as cyber patrols by civilian volunteers. To provide an activity space that calls for more advanced capabilities, aimed at cybersecurity engineers who possess a higher level of technical skills, the defense of cyberspace has been positioned as a social contribution activity for protecting the security of the country, and the government is leading efforts to establish pro-bono organizations with a focus on cybersecurity experts and IT engineers. Through such efforts, it is possible to build a system in which pro-bono cyber defense organizations cooperate with NISC to provide technical support to CII operators that have suffered damage, as a part of the response to large-scale cyberattacks on critical infrastructure.

The second policy is to enhance and utilize the SDF reserve personnel system in relation to cyber defense in the Ministry of Defense and Self-Defense Forces. Three systems are currently in place: the ready reserve personnel system, the reserve personnel system, and the reserve candidate personnel system. Reserve personnel and ready reserve personnel are engaged in various occupations in their private lives as working adults or students, and participate in training to maintain the necessary skills required by SDF personnel. They are mobilized through defense call-ups and disaster call-ups, and partake in activities as SDF personnel on these occasions. Under the current system, civilians who wish to become a reserve personnel, who can be expected to play an active role in the field of cybersecurity, and who hold official qualifications such as data processing specialist, are recruited in the "information processing" category under the reserve candidate personnel system (Technical). They undergo the necessary education and training for 10 days within a two-year period, and are appointed as reserve personnel after completing the training. Reserve personnel are called up through a defense call-up order, civilian protection call-up order, and disaster call-up order, and become SDF personnel when they are mobilized.[80] By engaging in activities as an SDF personnel under the orders of the commander of a cyber defense-related unit, they can acquire qualification as a combatant under international law rather than remain as civilians. However, the current education and training for reserve candidate personnel and reserve personnel focuses on common areas such as mental training, weapons training, basic training, and physical training. The education and training system for reserve personnel who are responsible for cyber defense should cover not only the common subjects that are the minimum requirements in basic training for SDF personnel, but should also be revised to focus on subjects with a strong connection to cyberwar, such as international law and the protection of confidentiality. At the same time, education and training should be implemented in the Cyber Defense Group and the systems defense units of each Self-Defense Force, and a system should be established to enable units specializing in cyberwar to respond swiftly in the event of an emergency.

By combining these two policies, Japan should be able to create a system close to the Cyber Defense Unit of Estonia. In short, civilians who wish to contribute to national defense in the

---

[79] National Police Agency, "Saiba Bohan Borantia Katsudo no Tame no Manyuaru (Moderu)" [Manual for Cyber Crime Voluntary Activities (Model)], http://www.npa.go.jp/cyber/policy/volunteer/manual.pdf.

[80] Ministry of Defense, "Heisei 30 Nendo Yobi Jieikanho Boshu Yoko (Gino Kobo)" [FY2018 Recruitment Guidelines for Reserve Candidate Personnel (Open Skills Recruitment)], http://www.mod.go.jp/gsdf/jieikanbosyu/pdf/ y/30yobihoginouy.pdf

area of cybersecurity can be encouraged to play an active role in voluntary activities related to cybersecurity as a member of the pro-bono cyber defense organization during peacetime, as well as serve as a member of the specialized cyberwar unit as an SDF personnel through defense call-ups during an emergency.

Conclusion

This paper examined, through a comparison with Estonia's cybersecurity policies, the cybersecurity policies that Japan has implemented to date, how public-private partnership initiatives on the protection of critical infrastructure have advanced, which policies are superior in comparison with other countries, which areas are lagging behind with regard to the implementation of measures, and which measures need to be implemented going forward.

Estonia drew lessons from the large-scale cyberattack that struck in April 2007, and has positioned the protection of vital services as the issue of highest priority in its cybersecurity strategy. The RIA consolidates the authority for the supervision of planning, formulating, and execution of cybersecurity policies, and strengthens regulations over vital service providers through the development of legal systems. Vital service operators are actively involved in national policies, and in addition to promoting security measures for information systems, also participate in various cyber exercises to contribute to the strengthening of the cybersecurity of Estonia as a whole. Furthermore, volunteer cybersecurity engineers who played an active role in the large-scale cyberattack incident in Estonia have become members of the Cyber Defense Unit under the Estonian Defense League, a paramilitary organization. While engaging in their day jobs, they wear the uniform of the Estonian Defense League and engage in national defense missions in cyberspace when a cyber incident occurs at the national level. In August 2018, the Cyber Command was newly established in the Estonian Defense Forces, and attention should be paid to the cooperative system that will be established by the Cyber Command, which is an arm of the regular army, and the Cyber Defense Unit, which is a paramilitary organization. Such public-private partnership initiatives in Estonia can be applied to Japan's cybersecurity policies.

Japan has, till now, steadily promoted cybersecurity policies. However, the means of cyberattacks are becoming increasingly ingenious and complex. To respond flexibly and swiftly to changes in the threats, it is important not only to utilize the latest cybersecurity technologies, but also to take reference from best practices promoted by Estonia to develop a public-private partnership system that corresponds with Japan's characteristics. In particular, during Prime Minister Abe's visit to Estonia in January 2018, Japan's participation in NATO CCDCOE was approved. On top of that, during the visit to Estonia by Defense Minister Onodera in May the same year, the dispatch of the defense ministry's staff to NATO CCDCOE was approved.[81] Going forward, in addition to promoting cooperation in the cyber field between Japan and Estonia through the dispatch of defense ministry staff, the acquisition of information locally about public-private partnership initiatives in the field of cyber defense in Estonia is also expected to be reflected in Japan's cybersecurity policies.

Cyberspace is a new theater of war. Unlike other domains, it is highly dependent on private-

[81] Ministry of Defense, "Esutonia Boeiso Kaidan (Gaiyo)" [Japan-Estonia Defense Ministers' Meeting (Summary)], http://www.mod.go.jp/j/approach/exchange/nikoku/docs/2018/05/06_j-estonia_gaiyo.pdf

sector actors. To achieve cyber defense for the country, there are limitations to the response that can be delivered by the government and military organizations alone. Hence, it is necessary to put tireless effort into cooperating with private-sector actors to realize “deterrence through resilience.”