CYBERDEFENSE REPORT

Estonia's National Cybersecurity and Cyberdefense Posture

Policy and Organizations

Zürich, September 2020

Cyber Defense Project (CDP)
Center for Security Studies (CSS), ETH Zürich

CSS ETH Zurich

ETH zürich

Available online at: css.ethz.ch/en/publications/risk-and-resilience-reports.html

Author: Kevin Kohler

ETH-CSS project management: Myriam Dunn Cavelty, Deputy for Research and Teaching; Benjamin Scharte, Head of the Risk and Resilience Team; Andreas Wenger, Director of the CSS.

Layout and graphics: Miriam Dahinden-Ganzoni
Editor: Sean Cordey

DOI: 10.3929/ethz-b-000438276

Table of Contents

1 Introduction

1.1 Report

The goal of this report is to provide the reader with a deeper understanding of the evolutionary path Estonia's national cybersecurity and cyberdefense posture has taken since 1991. To do so, the report outlines the trigger events, the major policy documents, and the current organizational structure. Please note that this report is non-exhaustive. Accordingly, there are numerous sectoral developments, specialized regulations, and smaller governmental organizations that this study does not specifically touch upon.

This first section introduces the Estonian geopolitical and historical context, both of which are the underlying drivers of its efforts in cyberspace. Section 2 describes the key focusing events that have shaped the Estonian threat perception and actions with regards to cyberspace. Section 3 outlines the national organizational framework and the responsibilities for the different cyber-related policy areas. Section 4 provides an overview of the current national strategic and legal documents. Section 5 expands the scope by looking at Estonia's international cooperation and partnerships. The study concludes with a discussion of the key themes in Estonia's cybersecurity and cyberdefense posture.

1.2 Background

Estonia is a small Baltic country (1.3 million inhabitants), which gained its independence from the Russian Empire in 1918, lost it to the Soviet Union in 1940, and regained it in 1991. Its northeastern border is about 150 kilometers away from St. Petersburg, the second-largest city in Russia. Estonia also has a significant Russian ethnic minority (24.8 per cent), which particularly concentrates in the northeastern Ida-Viru County and its largest city Narva, where ethnic Russians constitute a majority. The geopolitical reality of having such a powerful neighbor, which has historically refused to accept its sovereignty, has defined Estonia. The only way for Estonia to balance Russian influence has been through collective security arrangements; hence it is unsurprising that Estonia has eagerly joined in 2004 both the North Atlantic Treaty Organization and the European Union.

Similarly, the decision to make digitalization a key pillar of its development has some of its roots in the Soviet occupation. Following the independence, a young group of neoliberals won the first elections and strove to leave the Soviet legacies behind. The first post-independence Prime Minister, Mart Laar, was 32 when he assumed office, and his cabinet was equally young. His government decided early on to follow a leapfrog strategy to adapt to and work with the newest technologies rather than to modernize the heavy industry, which had been created by Moscow and was tied to ethnic Russians immigration (Kattel & Mergel, 2018, p. 5). Both of these factors, combined with the fact that Estonia has no large natural resources, help explain why Estonia embraced emerging ICT-technologies and digitalization. The most notable initiative in this regard is probably the 1996 Tiger's Leap (*Tiigrihüpe*) program to aggressively include computer science in education.

Today, Estonia has earned a reputation as one of the most highly digitalized societies in the world, in particular with regards to public digital infrastructure and e-identity. At the same time, this reliance on digital services also increases its exposure to cyberattacks. Estonia has particularly been the target of politically motivated cyberattacks from actors linked to Russia. In 2007, after the relocation of a Soviet-Era monument, Estonia was subject to a previously unseen level of distributed denial-of-service attacks that lasted for three weeks and targeted the Estonian parliament, banks, ministries, newspapers, and broadcasters. The attacks created little lasting damage; they, however, served as a powerful wake-up call. In the aftermath, Estonia became the first European country to pursue a comprehensive cyber policy approach through a national cybersecurity strategy and the creation of new dedicated bodies, such as the Estonian Defence League's Cyber Unit. Its capital Tallinn was notably selected to host the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Cybersecurity and cyberdefense have continued to be a high priority for Estonia ever since. In 2018 it established a Cyber Command within the Estonian Defense Forces (*Eesti Kaitsevägi,* EK), and in 2019 Estonia published the third iteration of its national cybersecurity strategy.

2 Trigger Events

This section describes the key international and domestic events that affected the perceived importance of cybersecurity in Estonia and helped shape its policies. Given the centrality of digitalization in its development, Estonia was naturally incentivized to put a higher priority on cybersecurity than other countries. However, **the origin of Estonia as a cybersecurity leader has a clear date: 27 April 2007**. The coordinated denial-of-service attacks (DDoS) against the infrastructure of Estonia mercilessly exposed the country's digital vulnerability. In the long run, the attacks turned out to be a blessing in disguise insofar as they have helped Estonia recognize and respond to the crucial importance of cybersecurity earlier than most countries. The subsequently listed events did not have the same level of impact. Still, they have helped to further sharpen and adjust Estonia's threat perception and approach to cybersecurity.

2.1 2007 Cyberattacks

Triggered by the relocation of a controversial Soviet-era bronze soldier from a small park in the center of Tallinn to the military cemetery on 27 April 2007, **Estonia experienced a series of politically motivated cyberattacks that lasted for twenty-two days**. The memorial had been erected in 1947 to commemorate the victory of the Soviet Army over Nazi Germany in WWII. However, for many Estonians, it came to symbolize the Soviet occupation and anti-Estonian extremists, who used it as a gathering place. On the evening of 26 April protesters gathered around the statue and attacked the police resulting in 100 injuries and one death. After that, the focus shifted to cyberspace.

Distributed denial-of-service attacks – of different levels of sophistication – against all types of critical or symbolic institutions were the most prominent kind of cyberattacks. Targets included the Estonian parliament, all ministries except the Ministry of Culture, and the free market liberal Reform Party of Foreign Minister Urmas Paet, whose website was defaced. Furthermore, three major internet service providers and three of Estonia's six largest news organizations suffered from DDoS attacks. Possibly the most serious attacks targeted, between 9 and 15 May, the e-banking infrastructure of Estonia's two largest banks; Hansapank and SEB Eesti Ühispank. This led to temporarily degraded services. In response, the Estonian banks had to cut off all inbound traffic into the country temporarily. A white list of countries from whom incoming traffic was accepted was then gradually expanded to countries with many clients but a low volume of malicious traffic. At the same time, youth groups physically besieged the Estonian embassy in Moscow. The Estonian ambassador was also physically attacked during a press conference on 2 May.

In the subsequent investigations, Russian officials refused to cooperate with their Estonian counterparts. The only individual that Estonian authorities were able to arrest and fine for taking part in the campaign was a young Estonian student of Russian ethnicity. However, the evidence points towards Russian nationals as the main attackers. Indications include the trigger event itself, the words in malformed queries, the defacements, the likely time zones of attackers, the attack instructions on Russian forums, the reactions, and the statements by Russian officials, such as Sergei Markov (Coalson, 2009). The attacks did arguably not constitute the first "cyber war," as claimed by Western news outlets at the time (Kaiser, 2015). Specifically, it did not reach the threshold of an armed attack, and there is no evidence for the direct involvement of Russian military or intelligence actors. The Russian state maintains that the attacks occurred without its involvement (BBC, 2007). However, Western observers concluded that it was more than just a spontaneous grassroots cyber riot. Ottis (2008) suggests understanding the attacks as a Russian information operation against Estonia, in which the government encouraged its citizens to attack (i.e. "people's war," "patriot hacking") while maintaining some level of deniability.

The 2007 cyberattacks have served as a powerful wake-up call highlighting Estonia's vulnerability and exposure to cyberattacks. In a meeting with then US President George W. Bush in June 2007, the Estonian President Toomas Hendrik Ilves publicly affirmed his commitment to turn Estonia into a leader in cybersecurity: "Estonia became famous at the end of the last century for its Tiger's Leap program, which resulted in the internetization of the country, and now we must seriously tackle the Tiger's Security program, which would safeguard us all from cyberattacks" (Office of the President, 2007). The main lessons that can be drawn from the attacks against Estonia include: a) the need for a comprehensive strategy approach; b) the threat of politically motivated cyberattacks; c) the need for legal reform; d) the importance of education; e) the need for intensified international cooperation; and f) the potential of including volunteers (Czosseck, Ottis & Talihärm, 2011, pp. 29-31).

In July 2007, the Estonian government approved an action plan to fight cyberattacks. (Kaska, Talihärm, & Tikk, 2010). In September, the government approved the revised implementation plan of the Estonian Information Society Strategy (MKM, 2007). In May 2008, the Estonian government **adopted its first national cybersecurity strategy,** which was a comprehensive policy response to the cyberattacks. The goals of the strategy were: to develop and implement on a large-

scale a system of security measures; to improve the legal framework; to increase skills; to bolster international cooperation, as well as to raise awareness on cybersecurity**.**

2.2 Russo-Georgian War

On 7 August 2008, Georgian forces launched an attack against separatist forces in the region of South Ossetia. Referring to his obligations to "protect Russian citizens abroad," Russian President Vladimir Putin responded by sending military troops into South Ossetia as well as into government-controlled Georgian territory. The five-day Russo-Georgian War was supplemented by cyberattacks – mainly DDoS and defacements – against Georgian institutions. In the first phase, attacks primarily focused on Georgian news and government websites. In the second phase, the attacks extended to financial institutions, businesses, educational institutions, and Western media. To avoid an information blockade, the Georgian government had to rely on allied host servers outside of the country. For example, Google allowed the site of the Georgian Ministry of Foreign Affairs to be hosted on blogger. Poland, meanwhile, redistributed Georgian press releases while Estonia hosted a server for the Georgian Ministry of Foreign Affairs. The latter also sent two specialists from the Estonian Computer Emergency Response Team (CERT-EE) to Georgia to assist the mitigation efforts.

While these attacks on Georgia have not directly led to any policy changes in Estonia, they again highlighted Moscow's willingness to tie the presence of ethnic Russians to military interventions, the threat of simultaneous cyberattacks against the websites of governing institutions, as well as the value of **cooperation with countries that are in a similar geopolitical situation**.

2.3 Annexation of Crimea

In the wake of the Euromaidan Revolution, the pro-Russian Ukrainian President Viktor Yanukovych fled to Russia on 22 February 2014. A pro-European government then replaced the former pro-Russian one. On 27 February, unmarked Russian troops invaded the Crimea peninsula, which has a Russian ethnic majority and hosts the Russian Black Sea Fleet in Sevastopol. After taking over strategic points and installing a pro-Russian government, Crimea held a blitz referendum, declared its independence on 16 March, and joined Russia on 18 March.

The sudden annexation of Crimea reminded Estonia of how it had lost its independence to the Soviet Union in June 1940. At the time, the Soviet Union had set up a military blockade and placed a large invasion force on the Estonian borders. Estonia was forced to accept the ultimatum to build a Soviet-friendly government. In July, rigged elections were held in which only Soviet-supported candidates were permitted to run. Citizens who failed to vote for a communist candidate risked their lives. The resulting communist parliament then immediately joined the Soviet Union.

An analysis commissioned by the Ministry of Finance in 2013 had already highlighted the need to ensure the cyberdefense of "digital monuments" (i.e. websites with symbolic statuses, such as president.ee), Estonia's digital continuity, and the functioning of the state in any emergency. However, the annexation of Crimea **brought to the forefront of political discussions the issue of ensuring the continuity of government and public services**. Estonia decided that it needed to develop capabilities outside of the country's borders and considered two options: a physical embassy for data in a friendly foreign country or a virtual embassy for data in a privately-owned public cloud. **In 2017, Estonia reached an agreement with Luxembourg to open the world's first "data embassy."** This allows the Baltic state to store its data in a physically separated compartment of data centers that operates under Estonian jurisdiction.

2.4 WannaCry and NotPetya

In 2017, two severe cyberattacks – i.e. the WannaCry ransomware (May) and the NotPetya ransomware/wiper (June) – hit the world. The cyberattacks are attributed to North Korea and the Russian foreign military-intelligence agency GRU, respectively. Both critically affected large organizations, such as the UK's National Health Service (WannaCry) or the world's largest container operator Maersk (NotPetya), causing massive economic costs. WannaCry is estimated to have caused damages worth between four and eight billion USD, while NotPetya about ten billion USD. Both attacks relied on the "Eternal Blue" exploit, which targets the Windows operating system. The National Security Agency (NSA) had initially developed "Eternal Blue," before the "Shadow Brokers" stole and subsequently leaked it in April 2017. NotPetya further combined it with the password-stealing malware Mimikatz. Importantly, Microsoft had already released patches before WannaCry to close the Eternal Blue exploit. **Hence**, **much of the spread of WannaCry was due to organizations that had not applied patches or were operating Windows systems that were past their end-of-life.**

WannaCry had no impact on Estonia. The Estonian Information System Authority (*Riigi Infosüsteemi Amet*, RIA) notes that the malware was detected in twenty systems, all of which already had a

security-patched operating system. NotPetya, meanwhile, had a limited impact on Estonia. It notably damaged the manufacturing company Saint-Gobain's Estonian subsidiaries, among them Ehituse ABC, which had to close all of its stores in the country. Consultancy Kantar Emor temporarily halted its information systems as a precaution as their parent company's network had experienced an infection. Estonia has attributed its relative success in dealing with WannaCry and NotPetya to both its readiness and rapid response. First, Estonia had started an awareness campaign to reduce reliance on the old Windows XP operating system as early as 2013 and was able to reduce the share of the operating system below 20 per cent. Second, Estonia immediately and pro-actively contacted institutions that were potentially endangered by WannaCry and NotPetya and advised them on systems protection (RIA, 2018, pp. 23-25). The high costs induced by these attacks on other economies have **affirmed Estonia's support to replace legacy services and solutions**. Estonia's third cybersecurity strategy is the first to explicitly mention the adherence to this "no-legacy" principle (Ministry of Economic Affairs and Communication, 2019, p. 38).

2.5 ROCA Vulnerability in eID

On 30 August 2017, a cryptography research group at Masaryk University in the Czech Republic notified CERT-EE of a security vulnerability in the chips used in its state-issued electronic identity cards (eID). The vulnerability, known as "the Return of the Coppersmith Attack (ROCA)," affected the cryptographic keypair generation in chips produced by Infineon, which was a supplier to Gemalto – i.e. the main supplier of the Estonian ID card. Theoretically, the ROCA vulnerability allowed the private key to be calculated from the public key. While doing so required significant expertise in cryptography and about 80,000 USD worth of computing power at that time, it was clear that the risk of exploitation would increase once the research group would publish their methodology. On 25 October Estonia began issuing new ID cards that relied on a different encryption algorithm and started testing the online updating of affected eIDs. On 30 October, the international group of cryptographers published their research. The next day, all eID holders were called on to update their cards online. Three days later, the certificates of 740,000 affected Estonian ID cards were blocked. They only became usable after their owner had updated it. By the end of 2017, 400,000 eIDs had been updated, and the service usage statistics showed no drop in the usage of digital services (RIA, 2018, p. 4). Overall, Estonia managed the vulnerability smoothly as it had the ability to remotely update its eID cards, which, as a precaution, already had several crypto libraries embedded in their firmware.

In its subsequent analysis of the incident, the RIA (2018, p. 3) highlighted gaps in the EU supply chain management and notification mechanism with regards to vulnerabilities that don't have a demonstrated impact yet. Estonia was particularly upset that Gemalto did not immediately inform the authorities. The Police and Border Guard Board (2018) has subsequently filed lawsuits against Gemalto and switched to a new supplier – i.e. Idemia – for the eID. RIA also **stressed the need to develop and integrate electronic alternatives to the ID card, as it didn't view traditional face-to-face authentication and handwritten signatures as acceptable secondary options**. Lastly, it reiterated the importance of broad-based cooperation between national, international and corporate stakeholders.

3 Organizational Structures

This section provides an overview (see Figure 1.) of the Estonian organizational structure, highlighting which institutions are responsible for the different cybersecurity and cyberdefense related policy areas.

3.1 Cybersecurity

Since 2011 the **Ministry of Economic Affairs and Communications (*Majandus-ja Kommunikatsiooniministeerium*, MKM)** is responsible for the general coordination of cybersecurity policy. The **Cyber Security Council of the Government Security Committee**, which brings together seven ministries and the government office, supports cross-departmental strategic cooperation and monitors the implementation of the cybersecurity strategy since 2009. The Permanent Secretary of the MKM heads the council and submits to the government an annual progress report on the realization of the targets set out in the strategy.

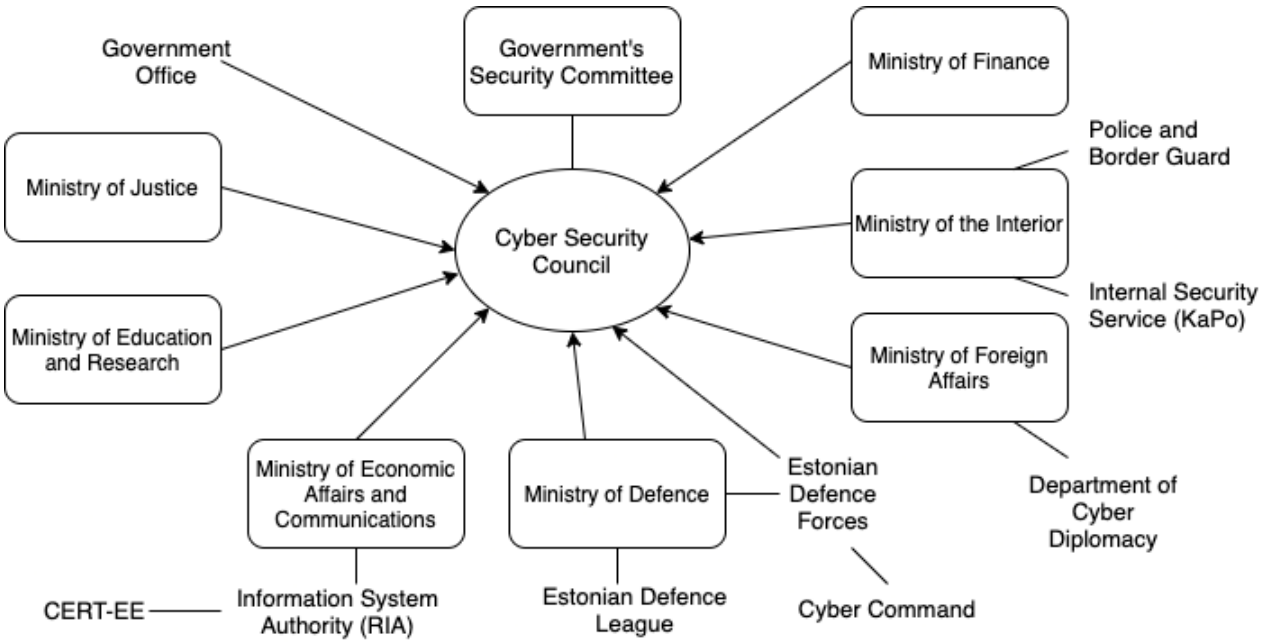
The **Estonian Information System Authority (*Riigi Infosüsteemi Amet*, RIA)** is the central cybersecurity competence and coordination body within the MKM. RIA is responsible for the development and management of the government's information systems, coordinating the implementation of security standards, and drafting related policies and strategies. RIA can conduct risk analyses of critical information infrastructures and impose extra-judicial fines for insufficient actions on operators of essential services or digital service providers.

Located within the RIA, the **Estonian Computer Emergency Response Team (CERT-EE)** is the national computer security incident response capacity and is operational 24/7. It reacts to cyber incidents in Estonian networks, provides warnings about malware and vulnerabilities, and manages the Estonian data exchange layer "X-Road" as well as the state portal "eesti.ee." CERT-EE also administers a virtual situation room that enables crisis coordination between service providers and government agencies. All significant cybersecurity incidents at state entities, operators of essential services, and digital service providers have to be reported to CERT-EE.

3.2 Cyberdefense

The **Ministry of Defense (*Kaitseministeerium*, KM)** is responsible for national defense, including cyberdefense. In February 2014, the KM launched the **Cyber Policy and Information and Communications Technology Department**, which specifically focuses on cyber policy and is administered by the Undersecretary for Legal and Administrative Affairs. The **Cyber Command** of the Estonian Defense Forces (EK), established in August 2018, is the main institution tasked with protecting cyberspace within the Ministry of Defense's governance area. The Cyber Command will achieve full operational capacity by 2023 and will consist of around 300 military and civil personnel in peacetime. 240 positions are to be transferred from existing units and 60 positions are to be newly created (Pernik, 2018). The overall personnel of the Estonian Defense Forces in peacetime is only about 6,000. Hence, the Cyber Command reflects a significant commitment and about five per cent of all the EK's personnel. The Cyber

Figure 1. Composition of the Cyber Security Council of the Government Security Committee.



Command has been built on the basis of the Headquarters Support and Signal Battalion and reports directly to the Commander of the EK (see figure 2.). In addition to information operations, it is responsible for providing ICT services, command support, and strategic communication. The protection of the ICT systems by the Defense Forces against cyber threats, as well as the planning and organization of cyber and information operations, take place within the Cyber and INFOOPS Center.

In addition to the KM, national cyberdefense is supported by the **Estonian Defence League's Cyber Defence Unit (EDL CDU)**, which includes cybersecurity professionals from both public and private entities. The Estonian Defence League is a voluntary defense organization with about 16,000 members. The Estonian Defence League Act of 2013 explicitly integrates the EDL CDU into the national defense system, with a framework for its structure, management, membership, and functioning (see Baezner, 2020).

3.3 Cybercrime

The cybercrime unit of the Police and Border Guard Board investigates cybercrimes and raises awareness regarding cyber threats. The Internal Security Development Plan 2015-2020 lays out the planning of activities related to the development of anti-cybercrime capabilities (Ministry of the Interior, 2014). The Ministry of Justice and its subordinate prosecutor's office apply the laws concerning cybercrimes.

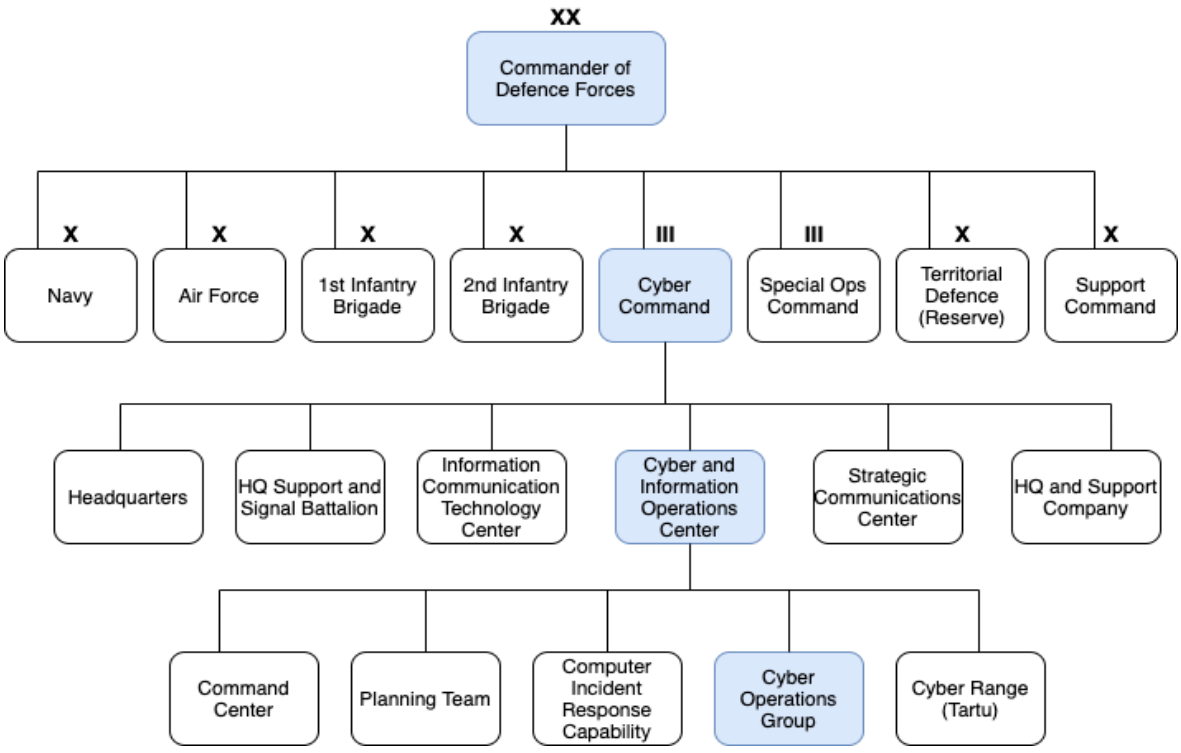
3.4 Cyberdiplomacy

In September 2018, Estonia appointed Heli Tiirmaa-Klaar, who was previously the head of cyber policy coordination at the European External Action Service (EEAS), as the country's first **Ambassador at Large for Cyber Security**. In September 2019, the Ministry of Foreign Affairs created the **Cyber Diplomacy Department** within the area of the Undersecretary for Political Affairs. The department contributes to sectoral discussions in international organizations, promotes bilateral and multilateral relations, and supervises sectoral development cooperation.

3.5 Crisis Management

Estonia's crisis management process is based on the 2009 Emergency Act. It establishes the Minister of the Interior as the chair of the national Crisis Committee. The last national summary of emergency risk assessments in 2013 has identified a large-scale cyberattack as a high risk (risk class C). The State of Emergency Act provides the basis, conditions, and procedure for the declaration of a state of emergency. The last nationwide emergency response exercise CONEX 2015 included a large-scale cyber incident as one of five sub-exercises (Ministry of the Interior, 2015, p. 77). In March 2020 Estonian Prime Minister Jüri Ratas declared a nationwide state of emergency due to COVID-19.

Figure 2. Command Structure for Cyber Operations by the Estonian Defence Forces.



3.6 Intelligence

The Estonian Internal Security Service (*Kaitsepolitseiamet*, KaPo) is responsible for detecting and preventing cyber threats deriving from cyber intelligence, political extremism, terrorism, and sabotage. It conducts intelligence and criminal investigations in cooperation with its national and international partners. The latest annual review highlights the threats of phishing mails, in particular related to the Gamaredon advanced persistent threat group, VPN firewall weaknesses, and a security vulnerability at the email provider mail.ee (KaPo, 2019, pp. 34-37).

4 Strategy

This section outlines the key national strategy documents for Estonia's cybersecurity and defense posture. The central piece is the whole-of-government National Cybersecurity Strategy (NCS), which has been integrated with the Information Society Strategy under the umbrella of the Digital Agenda 2020 for Estonia (MKM, 2018, p. 4). Several other sectoral strategies complement the NCS (see Figure 4).

4.1 Cybersecurity Strategy 2019-2022

Already in its third iteration, Estonia's current Cybersecurity Strategy covers the years 2019 to 2022. Its implementation is budgeted to cost 2.1 million EUR per year (MKM, 2018, p. 41). The strategy follows four fundamental principles (MKM, 2019, p. 10):

1) "We consider the protection and promotion of **fundamental rights and freedoms** as important in cyberspace as in the physical environment.
2) We see cybersecurity as an **enabler and amplifier of Estonia's rapid digital development**, which is the basis for Estonia's socio-economic growth. Security must support innovation, and innovation must support security.
3) We recognize the **security assurance of cryptographic solutions to be of unique importance for Estonia** as it is the foundation of our digital ecosystem.
4) We consider **transparency and public trust** to be fundamental for a digital society. Therefore, we commit to adhere to the principle of open communication."

The third principle, which discusses the importance of cryptographic solutions, should be understood as a response to the ROCA vulnerability in the eID. Compared to the previous two National Cybersecurity Strategies, the number of guiding principles has been reduced from eight to four. However, that doesn't mean that Estonia does not subscribe to its earlier principles anymore. For example, the earlier principle that cybersecurity is an integral part of national security has largely been operationalized through the establishment of the Cyber Command. Furthermore, earlier principles that have noted that cybersecurity can only be ensured through international cooperation with allies and partners, as well as that there is a need for social awareness of cybersecurity and individual responsibility, are still included as strategic objectives of the current strategy. An overview of the evolution of guiding principles of Estonia's cybersecurity strategies follows in Table 1.

Estonia's Cybersecurity Strategy 2019-2022 aims to achieve four strategic objectives:

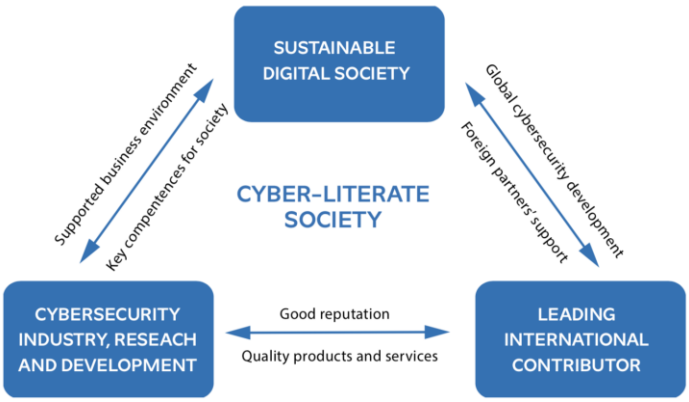
1) Build a sustainable digital society thanks to **strong technological resilience and emergency preparedness**.
2) Support and promote **research and development in cybersecurity** to foster a globally competitive industry.
3) Remain a **leading international contributor to cyber issues** with a reputation as a credible and capable partner.
4) Foster a **cyber-literate society** with high public awareness and a sufficient supply of talent.

Table 1. Guiding principles in the Cybersecurity Strategies of Estonia. Data from KM (2008, p. 7), MKM (2014, p. 7; 2019, p. 10)

Principles	**NCS I**	**NCS II**	**NCS III**
Protection of human rights / fundamental rights	■	■	■
Cybersecurity is an integral part of national security	■	■	
Multistakeholder approach with the private sector and civil society	■	■	
System owners/individuals should be aware of responsibilities	■	■	
International cooperation with allies and partners	■	■	
Private-public cooperation for CI protection	■		
Social awareness of cybersecurity	■		
Interoperable IT solutions in Estonia	■		
Principle of proportionality		■	
Anticipate as well as prevent potential threats		■	
Internationally competitive R&D		■	
Cybersecurity as an enabler and amplifier of digital development			■
Security assurance of cryptographic solutions of unique importance for Estonia			■
Transparency, public trust, open communication			■

As highlighted in Figure 3, these strategic objectives are interlinked, so that progress in one objective correlates positively with progress in other target areas.

Figure 3. The objectives and interrelations of the Cybersecurity Strategy. Reprinted from MKM (2019, p. 16).



The first objective is to ensure that Estonia is a **sustainable digital society with strong technological resilience and readiness to cope with crises**. This includes, amongst other things, adherence to information security and data protection principles, broad-based implementation of the Estonian ISKE baseline security requirements, and the systematic assessment and administration of risks related to next-generation technologies in fields such as cryptography, blockchain technology, artificial intelligence (AI), and secure identity management. The performance indicator for this objective is the **reduction of the total number of open services that are accessible to all internet users** in the state network as well as in the Estonian cyberspace to around a third of the starting levels.

The second objective – **of a globally competitive, research-based cybersecurity industry** – is measured through the export volume of the sector. It aims to roughly double the number of start-ups in that area and increase the number of doctorates awarded. The Estonian Information Security Association (EISA) is a cybersecurity cluster that supports cooperation between universities, businesses, and government. It aims to provide an administrative support mechanism for unified cross-sectoral participation in bidding on international contracts and competitions. Estonia's ICT development program and the IT academy program are the current measures related to promoting research and development. However, they are not entirely focused on cybersecurity, and preparations of a nationwide cybersecurity R&D plan that defines priority focus areas is underway. Lastly, there is cooperation between Startup Estonia and the Ministry of Defense. Estonia is also developing the Open Cyber Range platform, offering solutions to sectoral (start-up) companies and universities for carrying out R&D activities, testing, and training.

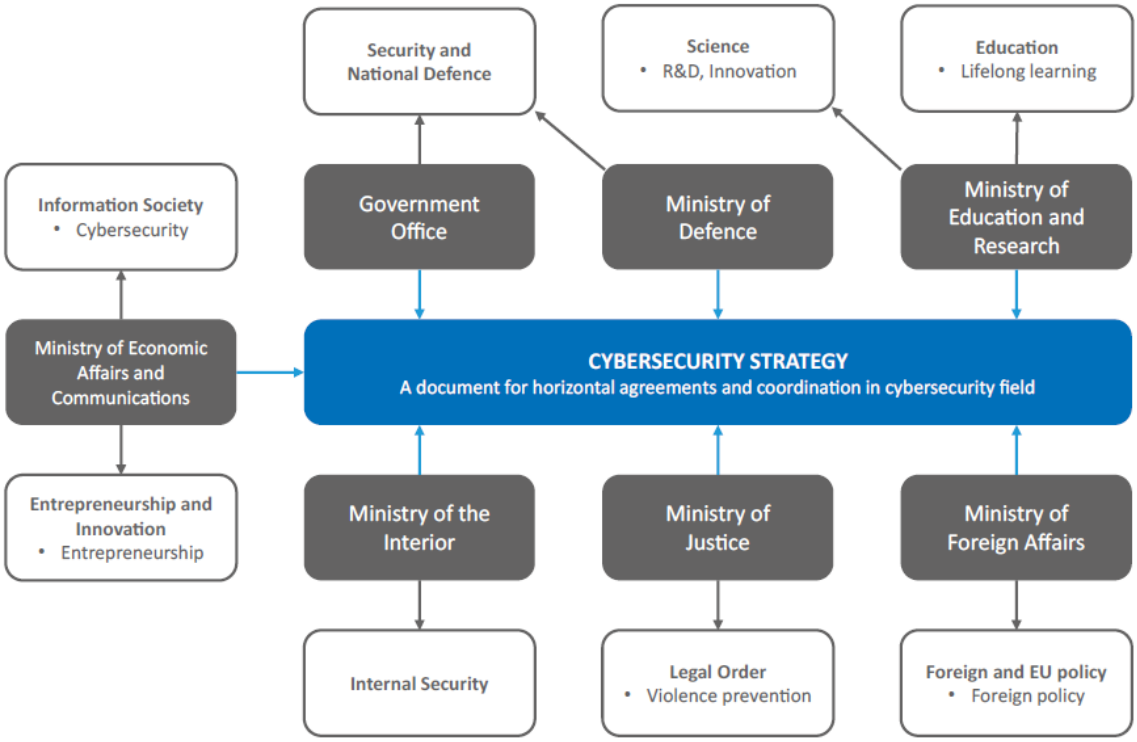
The third objective – that **Estonia is a credible and strong partner in the international arena** – is the hardest to assess in a quantifiable way. It is evaluated based on an annual expert assessment. The subgoals in this area are that **Estonia is sufficiently represented and has competence in cyber topics** at its representations to the EU, the UN, and NATO. It contributes to processes of shaping international law, develops bilateral cooperation formats with key partners, and regularly holds joint exercises. Furthermore, it makes active efforts to **strengthen the deterrence stances of the EU and NATO**. It also reinforces Estonia's active role in large-scale exercises, such as Locked Shields and Cyber Coalition. Lastly, Estonia aims to take part in **creating the EU cyber assistance network** and develop a competitive and sustainable cyber assistance provision capability.

The last objective is that **Estonia is a cyber-literate society, which guarantees a future supply of specialists**. The performance indicators for this objective include the share of Internet users aged 16-74 that have experienced one form of loss due to a security vulnerability online within one year. Estonia aims to bring this from 27.7 per cent in 2015 to below 20 per cent in 2020. It also seeks to increase the share of companies with an ICT security policy from 16.9 per cent to above 25 per cent as well as the share of government employees that perform satisfactorily in a newly required practical skills test to above 75 per cent.

In order to **increase awareness across the whole of society**, the knowledge and skills of students and teachers will be measured systematically, and a supply of training in the field of cybersecurity will be provided for general educational and vocational school teachers. So far, information on cybersecurity was spread out across different locations, such as the RIA blog, the Police and Border Guard Board website, or the *Targalt Internetis* project (for smarter Internet use by children and their parents). Now, a **systematic, nationwide platform** for government institutions and local governments for raising cyber awareness will be developed. The Cybersecurity Act that came into force in May 2018 gives the RIA a prevention and resolution coordinator role. Furthermore, the topic of **cybersecurity will be integrated into the state's mid-level and top leadership training** programs.

To create a pipeline of talents to meet state and private sector demand, a program of extracurricular activities for talented youths interested in cybersecurity will be created based on the Cyber Olympics model. This, in turn, will create a pool for finding people who will complete their military service in a cybersecurity field.

Figure 4. Strategies related to Cybersecurity in Estonia. Reprinted from MKM (2019, p. 32).



Conscription, meanwhile, would become a part of the cyberdefense educational path and a state recruitment platform. Furthermore, a systematic overview of the cyberdefense workforce needs will be created. The University of Tartu and TalTech continue to offer master's degrees in cyberdefense as well as competences in IT and technology law.

4.2 Digital Agenda 2020 for Estonia

This umbrella document includes the developments of the information society as well as cybersecurity. The general responsibility for the implementation of all activities lies with the MKM. The steering body for the strategy is the e-estonia council. However, the cybersecurity sub-strategy continues to be guided by the Cyber Security Council.

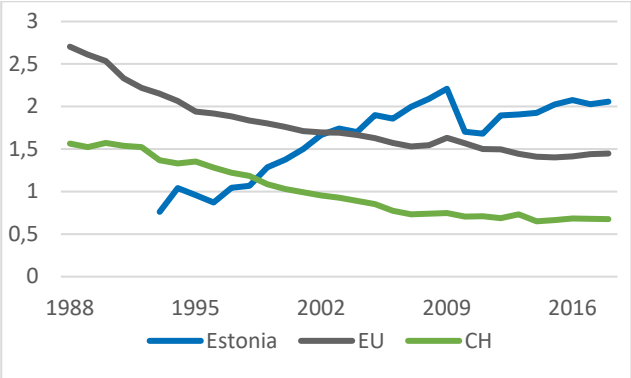
The five subgoals for the information society are (MKM, 2018. p. 11):

1) Access to fast Internet connections.
2) Basic infrastructure of a state information system enabling secure transmission of data.
3) The use of convenient and effective electronic services.
4) Better ICT skills for engaging in higher value-added work.
5) New business opportunities and exports.

4.3 National Defence Development Plan

The National Defence Development Plan 2017-2026 is Estonia's third ten-year plan. Previous ones covered the periods 2008-2017 and 2013-2022. It contains seven goals: the continuity of state and society, international security, strategic communication, internal security, support to the civilian sector, and military defense. Only a part of this document is publicly available. The plans to establish a Cyber Command are mentioned as part of achieving military defense (Government Office, 2017, p. 2). Goals include spending at least two per cent of GDP on military defense every year and to gradually increase the number of members of the Defence League to 30,000 without any specific target as to how many of them are allocated to the Cyber Unit (Government Office, 2017, p. 19). As such, Estonia is willing to invest more in defense than most European countries (see Figure 5).

Figure 5. Defense expenditures as a share of GDP for Estonia, EU, and Switzerland, 1988-2018. Data from World Bank, 2020.



4.4 Development Programs of the KM

The Development Plan of the Ministry of Defence 2020-2023 under the National Defence Development Program 2017-2026 includes four programs: Independent military defense capability, collective defense participation, intelligence, and advance warning, as well as defense policy design and supporting activities.

In terms of independent capabilities, the Cyber Command should be fully equipped and ready to serve as envisioned by the end of the development period. In terms of materials, a new mobile data center is being developed, a system for cross-defense communications is being tested, and a battle management system is being introduced (KM, 2020a).

In terms of collective defense, Estonia hosts the Allied Battle Forces Presence and NATO's Baltic Air Policing. Conversely, Estonia plans to continue to contribute to international military missions and operations based on solidarity with its Allies. In 2019, Estonia's largest contributions to international military operations were NATO Operation "Resolute Support Mission" in Afghanistan (42 members of the Estonian Defense Forces) and the French-led military operation "Barkhane" in Mali (48 members) (KM, 2020c).

In terms of supporting activities, the Ministry of Defense (2020b, p. 7) supports the annual "Cyber Olympics" organized by the Centre for Digital Forensics and Cyber Security at the Tallinn University of Technology since 2017. Furthermore, it supports a scholarship competition, prizes for the best graduation theses, and allocates grants to schools for teaching national defense. The goal is to raise the number of students participating from 5876 in 2019 to 6200 in 2022 (KM, 2020b, p. 9).

4.5 Foreign Policy Development Plan

The Foreign Policy Development Plan 2030 is the first long-term foreign policy strategy of Estonia with planned mid-term and ex-post evaluations. The strategy notes that the security, influence, and participation of a small country in international affairs depends more strongly on its reputation compared to large countries. Hence, Estonia's strengths and reputation in e-government, digital identity, e-services, and cybersecurity are central to its influence (Ministry of Foreign Affairs, 2019a, p. 12). Estonia aims to be an international cybersecurity advocate. It develops and strengthens cybersecurity in the EU, NATO, the UN, the Organization for Security and Co-operation in Europe (OSCE), and other international organizations. This includes strengthening the capacity of the European External Action Service to deal with cyber threats as well as working with like-minded nations globally to foster responsible behavior in cyberspace (Ministry of Foreign Affairs, 2019a, p. 17). Estonia further plans to develop comprehensive and in-depth cooperation with the United States, as a matter of priority, including cooperation on cybersecurity. In the Nordic-Baltic region, it invites countries to join the X-road secure data exchange layer (Ministry of Foreign Affairs, 2019a, p. 16).

4.6 Internal Security Development Plan

The Internal Security Development Plan 2015–2020 identifies ICT development as one of four major changes that are happening in the external environment. The others are international tensions in Eastern Europe, demographic changes, and continued globalization. The plan particularly highlights the need for cybercrime awareness, reliable and secure identity management, as well as the increased application of ICT for more efficient border management. As of 2015, 54 per cent of Estonia's land border was covered by electronic and technical surveillance. The goal is that by the end of the development plan, 90 per cent of the land border will be covered by electronic and technical surveillance (Ministry of the Interior, 2015, p. 16).

5 International Partnerships

This section looks at Estonian initiatives and agreements with key international organizations and partners.

5.1 European Union

Estonia is a member state of the European Union. The most important EU legislation on cybersecurity is the 2016 Network and Information Security (NIS) directive, which creates comparable national structures and establishes requirements – i.e. for security measures implementation and the notification of cyber incidents – for operators of essential services and digital service providers. **Estonia has transposed the NIS directive into national law in the 2018 Cyber Security Act**. Article 5 of the Cyber Security Act designates RIA as the national competent authority, the single point of contact, and the designated computer incident response team (CERT-EE) under the NIS Directive terminology.

Estonia held the rotating presidency of the Council of the European Union from July to December 2017 and has used it to promote progress on digital topics and **helped to prepare the European Union's cybersecurity strategy**. In September 2017, the Joint Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy laid out the fundamentals of the subsequent EU Cybersecurity Act. This includes a permanent mandate for the European Union Agency for Network and Information Security (ENISA) as well as an EU cybersecurity certification framework.

Furthermore, Estonia is part of the Permanent Structured Cooperation (PESCO), which pursues the structural integration of national armed forces. Within PESCO (2019), Estonia is part of the project to build **Cyber Rapid Response Teams and Mutual Assistance in Cyber Security**. The other members are Latvia, Croatia, the Netherlands, Poland, and Romania. Estonia is also part of the European Defence Agency's (EDA, 2018) Cyber Ranges Federation Project. In June 2018, it has also signed a Memorandum of Understanding (MoU) with Austria, Belgium, Finland, Germany, and Latvia on the **pooling and sharing of cyber range capabilities**. In November 2019, Estonia participated in the first live-fire exercise, in which the national cyber ranges of four participating countries and the European Space Agency were interconnected and interacting in real-time (EDA, 2019).

5.2 NATO

Estonia is a member of NATO. It had already recommended the creation of a new "center of excellence" for telecommunications security within the NATO framework in 2003, before even having joined the alliance (Jackson, 2013, p. 8). The Supreme Allied Commander Transformation approved the concept in 2006, and the 2007 attacks acted as a catalyst to push the idea forward. On 14 June 2007, at the first meeting of NATO defense ministers after the attacks, their joint communique noted: "In light of recent cyberattacks on one Ally's electronic infrastructure, urgent work is needed to enhance the ability to protect information systems of critical importance to the Alliance against cyber attacks (section 17)." Pursuant to this agreement, NATO conducted an assessment of its approach to cyberdefense and reported back to defense ministers in October 2007. In May 2008, Estonia established the **NATO Cooperative Cyber Defence Center of Excellence (CCDCOE)** with Germany, Italy, Latvia, Lithuania, Slovak Republic, and Spain as initial member states.

At the 2014 Wales summit, NATO recognized the validity of international law in cyberspace and declared that **cyberdefense is part of NATO's collective defense mandate**. At the 2016 Warsaw summit, NATO defined cyberspace as a new domain of military operations – comparable to air, land, and sea – in which the alliance must ensure its defense capabilities. Accordingly, in their Cyber Defense Pledge, the Allies committed to prioritizing enhancing the cyberdefenses of their national networks and infrastructures (NATO, 2016a).

At the Brussels Summit in 2018, Allies agreed to set up a new **Cyberspace Operations Centre** in Belgium as part of NATO's strengthened Command Structure. As of August 2019, the United States, United Kingdom, Denmark, the Netherlands, Estonia, Norway, Germany, France, Denmark, and Lithuania were the nine countries that have offered NATO national cyber capabilities to fight in cyberspace when necessary (Vavra, 2019).

Today, 22 NATO states sponsor the CCDCOE, and non-NATO states Austria, Finland, Sweden, Switzerland, Japan, and Australia are joining or have joined as contributing participants. The best-known accomplishment of the CCDCOE is the **Tallinn Manual on the International Law applicable to Cyber Operations**. Launched in 2009, with input from legal scholars and advisors from nearly 50 states, the Tallinn Manual process is by far the world's most comprehensive analysis of how existing international law applies to cyberspace. The first edition of the Tallinn Manual was published in 2013, the second edition in 2017.

Furthermore, the CCDCOE organizes the **annual multinational exercises Locked Shields and Crossed Swords**. The former is the largest and most complex international live-fire cyberdefense exercise in the world, which is run on the **NATO Cyber Range in Tartu operated by the EK**. Estonia has awarded a contract for building a next-generation cyber range that will be used by NATO (e-estonia, 2017), and it has initiated the Cyber Security Exercises and Training Centre CR14 to serve the needs of the cyber range.

5.3 United States

In 2013 the two countries signed the **US-Estonian Partnership Statement**, which includes technical cooperation between the Department of Homeland Security and RIA, collaboration on strategic engagement in international forums, such as the UN and NATO, as well as capacity-building with third-party countries (Ministry of Foreign Affairs, 2013). In 2019, the United States and Estonia concluded their third cyber dialogue. The two countries have started a **cooperation to build a joint platform for securely sharing cyber threat intelligence** between the US Department of Defense and the Estonian Ministry of Defense (e-estonia, 2020). This secure data exchange layer may later be opened to additional countries.

5.4 Others

United Nations. In 2004, the UN General Assembly established the Group of Governmental Experts (UN GGE) to examine the impact of developments in ICT on national security and military affairs. These groups have limited membership. However, Estonia has been a member of all of the six working groups except for the first one. Estonia has also been elected as a non-permanent member of the UN Security Council for the period of 2020 to 2021, and it has announced that e-governance and cybersecurity will be its top priorities. (Ministry of Foreign Affairs, 2019). In March 2020, Estonia has brought up the issue of cyberattacks on Georgia in the Security Council. Together with the United States and the United Kingdom, it attributes these attacks to the Russian GRU (Permanent Mission of Estonia to the UN, 2020).

Nordic-Baltic Cooperation (NB8). The Nordic-Baltic cooperation or NB8 is a regional cooperation format which was founded in 1992 and brings together five Nordic countries (Finland, Sweden, Norway, Iceland, Denmark) and three Baltic countries (Estonia, Latvia, Lithuania) to discuss regional and international issues. Since 2014, the NB8 and the United States have an annual roundtable on cybersecurity issues within the format of the Enhanced Partnership in Northern Europe (e-PINE). Estonia is chairing the NB8 in 2020 and has defined regional security, cyber cooperation, climate change, as well as cultural and health cooperation as its priorities.

OSCE. Estonia is a member of the Organization for Security and Co-operation in Europe (OSCE). On the issue of cybersecurity, the most relevant aspect is the confidence-building measures aimed at reducing conflict stemming from the use of information and communication technologies (OSCE, 2013).

CoE. Estonia is a member of the Council of Europe (CoE) and has signed and ratified the Budapest Convention on Cybercrime.

OECD. Estonia became the first Baltic state to join the Organisation for Economic Co-operation and Development (OECD) in 2010. Latvia followed in 2016 and Lithuania in 2018.

Further agreements. Estonia, inter alia, engages in cyber-related bilateral discussions, cooperation, or agreements with the Organization of American States (2014), the Netherlands (Ministry of Foreign Affairs, 2015), Japan (e-estonia, 2016), the Republic of Korea (KM, 2017), Iceland (Ministry of Foreign Affairs, 2017), the Republic of Mauritius (2017), and Singapore (KM, 2018). Luxembourg has agreed to host **the world's first data embassy**. This agreement allows the Estonian government to physically store sensitive data in a data center in Luxembourg whilst maintaining jurisdiction (Republic of Estonia, 2017). Estonia is backing up ten data sets in the data embassy: e-file (court system), treasury information system, e-land registry, taxable person's registry, business registry, population registry, State Gazette, identity documents registry, land cadastral registry, and national pension insurance registry (e-estonia, 2019).

6 Conclusion

After reviewing the key documents of Estonia's cybersecurity and cyberdefense posture, this final section provides a discussion of some of the key themes that help understand Estonia's relative influence and success in this area.

Strategic coherence. In the late 1990s and early 2000s, in part driven by the European Union accession process, Estonia experienced a mushrooming of sectoral strategies – over 120. Since then, Estonia has actively worked towards increasing the coherence between and effectiveness of its various strategies (OECD, 2015, pp. 67-69). In 2005, the government adopted a decree on strategic planning to harmonize the strategy-generation system and establish clear links between sector development and budgeting. In 2006, a strategy unit was established within the Government Office to exercise quality control over all government-wide strategies. Hence, today, Estonia's strategic planning includes two aspects that are not yet equally present in some other countries. First, Estonia tries to take high-level principles and objectives and turn them into specific, measurable, achievable, realistic, and timely performance indicators. Second, Estonia consistently highlights related sectoral strategies in its plans and has also worked to more strongly integrate its Information Society and Cybersecurity Strategies.

Hiding hand. While Estonia has a cybersecurity strategy of high-quality, it would be misleading to attribute most of its digital success to top-down planning. Rather the first impetus for digitalization came from informal convictions and utopian visions of young leaders. Kattel and Mergel (2018) explain it through the concept of the "hiding hand." It describes initiating visionary change without anticipating related challenges and risks. Due to unexpected learning and creativity during the process, this approach can lead to success. Whereas the idea of being the world's first country to try out anything can sound horrifying to entrenched and risk-averse bureaucracies, Estonia has tended to "just do it." Estonia was one of the world's first countries to strongly integrate computers into education, resulting in high levels of digital literacy in many decentral, bottom-up initiatives. Estonia was also the first country to adopt an electronic identity that almost all public services use, including voting. Estonia adopted the first European whole-of-government cybersecurity strategy, and it recently opened the world's first "data embassy." Estonia tends never to look back, even when something goes wrong. The 2007 cyberattacks were seen as a wake-up call for more cybersecurity, not for less digitalization. Similarly, RIA's (2018b, p. 3) response to the ROCA vulnerability has not been to ensure that there remains an analog alternative to all digital infrastructures, as it is, for example, advocated by Geer (2018). Rather it indicates a "digital first, digital second" strategy with the goal of developing digital alternatives to regular digital services with uncorrelated vulnerabilities. Audacity cannot easily be procured or planned for in a strategy.

Commitment and frugality. Estonia fulfills the NATO target of spending two per cent of GDP on defense. At the same time, it still has limited financial capabilities compared to other Western countries. Hence, it is sensitive to the cost-effectiveness of programs. When it comes to procurement for public services, Estonia has often favored open-source systems. The Baltic Defence College is an example of multinational burden sharing, and the EDL CDU is an example of maintaining surge capabilities for a (cyber-) crisis without very high costs.

Collective defense. Given its geopolitical context, Estonia relies on collective security and **strong partnerships with NATO, the EU, and the US**. Within these organizations, Estonia is a consistent advocate for **enhanced cooperation in cybersecurity and a strong stance on deterrence**. In turn, Estonia is supporting its allies even though it has no direct interests at stake in places like Mali or Afghanistan. However, the greatest value that Estonia provides to larger organizations may be that it provides infrastructure and impetus for cooperation, such as through organizing common exercises or bringing together legal experts for a mapping process.

Norm entrepreneur. Small states are generally interested in promoting and strengthening international norms of conduct. Neutral states, in particular, have often acted as peace brokers. However, Estonia does not aim to act as an impartial platform for great power discussions, but rather as an advocate and enabler of cooperation amongst like-minded nations (Crandall & Allan, 2015). Estonia regularly engages in public attributions of cyberattacks and has been very consistent in advocating for a free and secure Internet across time and forums, with a particular focus on NATO and the EU. Crandall and Allan (2015, p. 354) particularly note the consistent activism of the Fourth Estonian President Toomas Hendrik Ilves (2006-2016), who has used speeches at universities, international conferences, international organizations, discussions with other political leaders, and international working groups as venues that provide access to elites who are important in the norm promotion process.

7 Annex: Abbreviations

Abbreviations	English	Estonian
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence	n/a
CERT-EE	Computer Emergency Response Team - Estonia	n/a
CoE	Council of Europe	n/a
DDoS	Distributed Denial-of-Service	n/a
e-PINE	Enhanced Partnership in Northern Europe	n/a
EDA	European Defence Agency	n/a
EDL CU	Estonian Defense League's Cyber Unit	Kaitseliidu küberkaitse üksus
eID	Electronic identity	n/a
ENISA	European Network and Information Security Agency	n/a
EK	Estonian Defense Forces	Eesti Kaitsevägi
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation	n/a
ICT	Information and communication technology	n/a
ISKE	Estonian three-level IT baseline security system	Infosüsteemide Kolmeastmeline Etalonturbe Süsteemi
KaPo	Estonian Internal Security Service	Kaitsepolitseiamet
KM	Estonian Ministry of Defense	Kaitseministeerium
MKM	Estonian Ministry of Economic Affairs and Communications	Majandus- ja Kommunikatsiooniministeerium
NB8	Nordic-Baltic Eight / Nordic-Baltic Cooperation	n/a
NCS	National Cybersecurity Strategy	n/a
NIS	Network and Information Security	n/a
OECD	Organization for Economic Co-operation and Development	n/a
OSCE	Organization for Security and Co-operation in Europe	n/a
PESCO	Permanent Structured Cooperation	n/a
RIA	Information System Authority	Riigi Infosüsteemi Amet
ROCA	Return of the Coppersmith Attack	n/a
VPN	Virtual private network	n/a

8 Bibliography

Baezner Marie, *Study on the use of reserve forces in military cybersecurity* (Zürich: CSS/ETH, 2020).

BBC, "The cyber raiders hitting Estonia," *BBC,* 17.05.2007. http://news.bbc.co.uk/2/hi/europe/6665195.stm

Coalson Robert, "Behind the Estonia Cyberattacks," *RadioFreeEurope,* 06.03.2009. https://www.rferl.org/a/Behind_The_Estonia_Cyberattacks/1505613.html

Crandall Matthew, & Allan Collin, "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms," *Contemporary Security Policy,* (2015), pp. 346-368.

Czosseck Christian, Ottis Rain, & Talihärm Anna-Mariam, "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *Journal of Cyber Warfare and Terrorism*, 1:1 (2011), pp. 24-34.

E-estonia, *Estonia and Japan to Cooperate on Cyber Security*, e-estonia.com, 2016. https://e-estonia.com/estonia-and-japan-to-cooperate-on-cyber-security/

E-estonia, *Guardtime awarded contract for next-generation NATO Cyber Range, e-estionia.com,* 2017. https://e-estonia.com/guardtime-awarded-contract-for-next-generation-nato-cyber-range/

E-estonia, *Data Embassy – the digital continuity of a state,* e-estonia.com, 2019. https://e-estonia.com/data-embassy-the-digital-continuity-of-a-state/

E-estonia, *Estonia and the United States to build a joint cyber threat intelligence platform*, e-estionia.com, 2020. https://e-estonia.com/estonia-united-cyber-threat-intelligence-platform/

EDA, *Six Member States agree to pool & share cyber ranges capabilities*, eda.europa.eu, 2018. https://www.eda.europa.eu/info-hub/press-centre/latest-news/2018/06/28/six-member-states-agree-to-pool-share-cyber-ranges-capabilities

EDA, *EDA Cyber Ranges Federation project showcased at demo exercise in Finland,* eda.europa.eu, 2019. https://www.eda.europa.eu/info-hub/press-centre/latest-news/2019/11/07/eda-cyber-ranges-federation-project-showcased-at-demo-exercise-in-finland

European Parliament & Council of the European Union, *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Geer Dan, "A Rubicon," *Hoover Working Group on National Security, Technology, and Law* 1801 (2018).

Government Office, "Riigikaitse Arengukava 2017–2026 [National Defense Development Plan 2017-2026]," *Estonian Government Office*, (2017). https://www.riigikantselei.ee/sites/default/files/content-editors/Failid/rkak_2017_2026_avalik_osa.pdf

Information System Authority, "Summary of the Estonian Information System's Authority on Ensuring Cyber Security in 2012," *Information System Authority,* 2013. https://www.ria.ee/sites/default/files/content-editors/kuberturve/eisa_on_cyber_security_2012.pdf

Information System Authority, "2013 Annual Report: Cyber Security Branch of the Estonian Information System Authority," *Information System Authority,* 2014. https://www.ria.ee/sites/default/files/content-editors/kuberturve/2013-annual-report-cyber-security-branch.pdf

Information System Authority, "2014 Annual Report: Cyber Security Branch of the Estonian Information System Authority," *Information System Authority*, 2015. https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria-kyberturbe-aruanne-2014_eng.pdf

Information System Authority, "2015 Annual Report: Cyber Security Branch of the Estonian Information System Authority," *Information System Authority,* 2016. https://www.ria.ee/sites/default/files/content-editors/kuberturve/2015-ria-annual-cyber-report.pdf

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

Information System Authority, "Annual Cyber Security Assessment 2018," *Information System Authority,* 2018a. https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria-csa-2018.pdf

Information System Authority, "ROCA Vulnerability and eID: Lessons Learned", 2018b. https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf

Information System Authority, "Annual Cyber Security Assessment 2019," *Information System Authority,* 2019. https://www.ria.ee/sites/default/files/content-editors/kuberturve/ktt_aastaraport_eng_web.pdf

Kaiser Robert, "The birth of cyberwar," *Political Geography,* 46 (2015), pp. 11-20.

Kattel Rainer & Mergel Ines, "Estonia's digital transformation: Mission mystique and the hiding hand," *UCL Institute for Innovation and Public Purpose Working Paper Series* (IIPP WP 2018-09), 2018. https://www.ucl.ac.uk/bartlett/public-purpose/wp2018-09

Kaitseministeerium, "Cyber Security Strategy," *Kaitseministeerium*, 2008. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy/@@download_version/993354831bfc4d689c20492459f8a086/file_en

Kaitseministeerium, "Estonia and South Korea agreed on cyber cooperation*", Kaitseministeerium,* 2017. https://www.kaitseministeerium.ee//en/news/estonia-and-south-korea-agreed-cyber-cooperation

Kaitseministeerium, "Estonia and Singapore concluded a cyber cooperation agreement," *Kaitseministeerium, 2018.* https://www.kaitseministeerium.ee/en/news/estonia-and-singapore-concluded-cyber-cooperation-agreement

Kaitseministeerium, "Iseseisev sõjaline kaitsevõime [Independent military capabilities]", *Kaitseministeerium*, 2020a. https://kaitseministeerium.ee/sites/default/files/sisulehed/eesmargid_tegevused/2020_iseseisev_sojaline_kaitsevoime_kam_programm_1.pdf

Kaitseministeerium, "Kaitsepoliitika kujundamine ja toetav tegevus [Defence policy design and supporting activities]," *Kaitseministeerium,* 2020b. https://kaitseministeerium.ee/sites/default/files/sisulehed/eesmargid_tegevused/2020_kaitsepoliitika_kujundamine_ja_toetav_tegevus_kam_programm_4.pdf

Kaitseministeerium, "Kollektiivkaitses osalemine [Participation in collective defence]," *Kaitseministeerium*, 2020c. https://kaitseministeerium.ee/sites/default/files/sisulehed/eesmargid_tegevused/2020_kollektiivkaitses_osalemine_kam_programm_2.pdf

Majandus-ja Kommunikatsiooniministeerium, "2014-2017 Cyber Security Strategy," *Majandus-ja Kommunikatsiooniministeerium,* 2014. https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

Majandus-ja Kommunikatsiooniministeerium, "Digital Agenda 2020 for Estonia: Updated 2018 (Summary)," *Majandus-ja Kommunikatsiooniministeerium,* 2018. https://www.mkm.ee/sites/default/files/digital_agenda_2020_web_eng_04.06.19.pdf

Majandus-ja Kommunikatsiooniministeerium, "2019-2022 Cybersecurity Strategy", *Majandus-ja Kommunikatsiooniministeerium,* 2019. https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Ministry of Foreign Affairs, "U.S.-Estonian Cyber Partnership Statement," Ministry *of Foreign Affairs*, 2013. https://vm.ee/sites/default/files/content-editors/S-Estonian%20Cyper%20Partnership%20Statement.pdf

Ministry of Foreign Affairs, "Estonia and the Netherlands intensify cooperation in the cyber sphere," *Ministry of Foreign Affairs*, 2015. https://vm.ee/en/news/estonia-and-netherlands-intensify-cooperation-cyber-sphere

Ministry of Foreign Affairs, "Estonia ready to share cyber security expertise with Iceland", *Ministry of Foreign Affairs*, 2017. https://vm.ee/en/news/estonia-ready-share-cyber-security-expertise-iceland

Ministry of Foreign Affairs, "Eesti Välispoliitika Arengukava 2030 [Estonian Foreign Policy Development Plan 2030]," *Ministry of Foreign Affairs, 2019a.* https://vm.ee/sites/default/files/Estonia_for_UN/Rasmus/vpak_08.08.19_ak_marketa.pdf

Ministry of Foreign Affairs, "Foreign Minister Reinsalu: membership of the UN Security Council makes Estonia greater on the world map," *Ministry of Foreign Affairs*, 2019b. https://vm.ee/en/news/foreign-minister-reinsalu-membership-un-security-council-makes-estonia-greater-world-map

Ministry of the Interior, "Siseturvalisuse arengukava 2015–2020 [Internal Security Development Plan 2015-2030]," *Ministry of the Interior*, 2014. https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/taiendatud_siseturvalisuse_arengukava_2015-2020.pdf

NATO, *"*Final Communiqué: Meeting of the North Atlantic Council in Defence Ministers Session*," NATO*, 14.06.2007. https://www.nato.int/cps/en/natolive/news_47011.htm

NATO, "Wales Summit Declaration," *NATO*, 05.07.2014. https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO, "Cyber Defence Pledge," *NATO*, 08.07.2016. https://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO, "Warsaw Summit Communiqué," *NATO,* 09.07.2016b. https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

OECD, *OECD Public Governance Reviews: Estonia and Finland: Fostering Strategic Capacity across Governments and Digital Services across Borders*, (Paris:

OECD Public Governance Reviews/OECD Publishing, 2015). http://dx.doi.org/10.1787/9789264229334-en

Office of the President, "President Ilves met with the President of the United States," *Office of the President,* 24.06.2017. https://vp2006-2016.president.ee/en/media/press-releases/1440-president-ilves-met-with-the-president-of-the-united-states/index.html

Organization of American States, "OAS and Estonia Sign Cooperation Agreement on Cyber Security," *Organization of American States,* 20.10.2014. https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-445/14

OSCE, "Permanent Council Decision No. 1106," *OSCE, 2013*. https://www.osce.org/pc/109168

Ottis Rain, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," *Proceedings of the 7th European Conference on Information Warfare and Security*, 2008, pp. 163-168.

Permanent Mission of Estonia to the UN, "Stakeout on cyber-attack against Georgia by Estonia, the United Kingdom and the United States," *Permanent Mission of Estonia to the UN*, 05.03.2020. https://un.mfa.ee/press-stakeout-by-estonia-the-united-kingdom-and-the-united-states-on-cyber-attack-against-georgia/

Pernik Piret, "Preparing for Cyber Conflict: Case Studies of Cyber Command," *International center for Defence and Security,* 2018. https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf

PESCO, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security," *PESCO,* 2019. Retrieved from https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/

Police and Border Guard Board, "PPA esitas kohtule uue hagiavalduse Gemaltolt leppetrahvi nõudmiseks [The PBGB filed a new lawsuit against Gemalto for a contractual penalty]," *Police and Border Guard Board,* 06.09.2018. https://www.politsei.ee/et/uudised/ppa-esitas-kohtule-uue-hagiavalduse-gemaltolt-leppetrahvi-noudmiseks-222

Republic of Estonia, "Estonia to establish the world's first data embassy in Luxembourg," *Republic of Estonia,* 20.06.2017. https://www.valitsus.ee/en/news/estonia-establish-worlds-first-data-embassy-luxembourg

Republic of Mauritius, "Mauritius and Estonia sign MoU on Digital Cooperation," *Republic of Mauritius,* 30.11.2017. http://www.govmu.org/English/News/Pages/Mauritius-and-Estonia-sign-MoU-on-Digital-Cooperation-.aspx

Shlapak David, & Johnson, Michael, "Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defence of the Baltics", *RAND Corporation,* 2016. https://www.rand.org/pubs/research_reports/RR1253.html

World Bank. "Military expenditure (% GDP) - Estonia, Switzerland, European Union," *World Bank,* 2020. https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS?end=2018&locations=EE-CH-EU&start=1988

Statistics Estonia, *Population by ethnic nationality,* 01.01.2019. https://www.stat.ee/34278

Vavra Shannon, "NATO cyber-operations center will be leaning on its members for offensive hacks," *Cyberscoop,* 30.08.2019. https://www.cyberscoop.com/nato-cyber-operations-offensive-hacking-neal-dewar/

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.