5

Cybersecurity Lessons from Estonia

Heaven SULLIVAN

Abstract: Estonia is an excellent country to reference for cybersecurity lessons because of the country's long history and global reputation for expertise in the field. There are three aspects of Estonia's cybersecurity ecosystem that those hoping to learn from the country should examine. First is Estonia's heightened perception of cybersecurity's importance stemming from its post-Soviet restructuring, start-ups, and Russian threat. In general, this aspect is not replicable. The second aspect is cyber deterrence through international cooperation, which has limited replicability in European countries and other regions of the world. The third aspect is national cybersecurity agendas with specific and achievable goals. This aspect, with all it encompasses, can be replicated in a wide range of countries with varying economies and existing cybersecurity capabilities.

Key Words: Estonia, Cybersecurity, Replicability, e-Governance, Cyber deterrence

Introduction

Estonia is a small state on the Baltic Sea bordering Russia. In 1941 it was occupied by the Soviet Union and lost its sovergnty for nearly 40 years. Today the country is known for its elite e-governance and cybersecurity, becoming a leader in those fields since gaining its independence. This paper seeks to understand what Estonia's cybersecurity strategy is and identify those aspects that are replicable in other countries. In particular, this paper identifies and will focus on three distinct aspects of Estonia's cybersecurity strategy – a heightened perception of cybersecurity's importance, international cooperation in the European Union (EU) and North Atlantic Treaty Organization (NATO), and national cybersecurity agendas with specific and achievable goals.

Heightened Perception of Cybersecurity's Importance

Although most governments around the world recognize the importance of cybersecurity, Estonia is unparalleled in the importance placed on cybersecurity in its national identity, lifestyle, and economy. First, Estonia has an e-governance system that digitizes almost all of its citizen's data. For this system to work, that data must be adequately protected. Second, cybersecurity makes up a large part of Estonia's economy – the country leads Europe in start-ups, unicorns, and investments per capita.[274] Third, Estonia's expertise in cybersecurity increases its presence and influence on the global stage. Fourth, Estonia faces a unique and persistent cyber threat from neighboring Russia. This section concludes with an explanation of why this aspect of Estonia's cybersecurity strategy in not replicable in other countries.

[274] See https://investinestonia.com/estonia-leads-europe-in-startups-unicorns-and-investments-per-capita/ for more information on Estonian start-ups and economy.

E-Governance

Estonia's path to e-governance began when the country gained independence from the Soviet Union in 1991. (E-governance refers to the application of Information and Communication Technologies (ICT) for delivering government services.) The Soviet command economy and isolation from modern technologies behind the Iron Curtain left Estonia's economy and infrastructure in shambles. However, Estonian policy makers quickly realized that building an e-governance system from scratch was a unique opportunity. They sought to build new technological infrastructures from nothing while catching up with the West as quickly as possible. This led to a series of e-governance policies, online services, and internet initiatives that are presented in Figure 1.

Particularly important is the ambitious Tiger Leap Initiative launched in 1996 that aimed to build technology infrastructure by providing internet access to all schools in Estonia. The program was built on three pillars – "Computers and Internet, basic teacher training, and native-language electronic courseware for general education institutions."[275] The goal of the Tiger Leap Initiative was met in 2001 and laid the foundation for other important initiatives such as the Tiger Leap Plus, SchooLife, ProgeTiger, and the IT Academy. Together, these programs have built a digitally competent and technology focused society. Soon the goal would shift from building technology infrastructure to protecting the one that exists (i.e., cybersecurity).

Estonia has continued to develop its e-governance system, and cybersecurity not only became a digital necessity but also deeply infused into Estonian identity. In 2008, it developed a national e-Health system integrating data from Estonia's healthcare providers to improve the quality and efficiency. Similarly in 2010 e-Prescription was introduced, followed by e-Residency and the Road Administrations e-portal in 2014. Today 99% of public services are accessible online and the entire country has access to free public Internet.[276] Needless to say, life for Estonians is digital, and therefore needs

---

[275] Education Estonia, "How it all began? From Tiger Leap to digital society," 2022.

[276] *See* https://e-estonia.com/story/ for more information on e-governance in Estonia.

to be protected from cyberattacks and data breaches. This digital lifestyle has thus become an integral part of Estonian identity as former advisor to the Estonian Prime Minister of ICT, Linnar Viik, points out: "For other countries, the Internet is just another service, like tap water, or clean streets. But for young Estonians, the Internet is a manifestation of something more than a service – it's a symbol of democracy and freedom."[277] This sentiment is reflected by Estonia's development of the world's first data embassy in 2017. The embassy, which lies outside of Estonia's border in Luxembourg, assures the digital continuity of Estonian statehood in worst-case scenarios like critical system failures or external threats.

Economy

Estonia's boom in Internet infrastructure led to an innovative environment that fostered start-ups and helped rebuild Estonia's economy. In the 1990s, rules for private enterprises were simplified, a more transparent tax system was introduced, and communication with authorities was improved, resulting in a robust start-up network.[278] The culmination of this network happened in 2005, when the well-known Estonian start-up Skype was sold for $2.6 billion USD. One of the founders of Skype, Jane Tallinn, points out that start-ups in the early 2000s allowed the creation of a new class of Estonian investors. To date, Estonia has the most start-ups per capita in the world and has produced 10 start-ups with a value of over $1 billion USD (also known as unicorns.) Additionally, Estonia leads Europe in investments per capita.

Cybersecurity is essential to producing Estonia's start-ups and managing its investments. There are two major reasons for this. First, the security of its e-governance system allows Estonian start-ups and technology companies to utilize digital signatures, paperless communication, and online tax returns with ease. Second, strong and reliable cybersecurity practices provide trust to those buying start-ups and funding investments. Therefore,

---

[277] Patrick Kingsley, "How tiny Estonia stepped out of the USSR's shadow to become an internet titan," *The Guardian*, 2012.

[278] Katarzyna Kaminska-Korolczuk, and Barbara Kijewska, "The History of the Internet in Estonia and Poland," In *The Routledge Companion to Global Internet Histories*, edited by Gardard Goggin and Mark McLelland, 135–150. New York: Routledge, 2017.

an event such as a cyberattack or data breach could decrease trust in Estonian technology and comprise its economy more so than a similar event in other countries. This type of event would also diminish Estonia's shining role as a global cybersecurity leader and pioneer.

Global Presence

Estonia has emerged as a regional and global leader of cybersecurity, increasing its presence and power on the global stage. For example, Tallinn, the capital of Estonia, is home to NATOs Cooperative Cyber Defense Center of Excellence (CCDCOE) and was ranked the #1 country for cybersecurity in the EU in 2020.[279] Additionally, non-EU and non-NATO states also seek cybersecurity expertise from Estonia – as evidenced in 2019 when three Azerbaijani officials visited Estonia to learn and discuss Estonia's development and implementation of legislation of Internet technologies and study Estonia's cybersecurity strategies overall.[280]

Estonia's global leadership in cybersecurity is a result of several events, including Estonia's successful e-governance system, its reliable and innovative start-ups, the country's response to the 2007 cyberattacks on its infrastructure, its national goal to become a global leader in cybersecurity, and its success in deterring and minimizing cyberattacks. It is important to note that, compared to other global leaders in the field such as the United States, India, and China, being a global cybersecurity leader is far more important to Estonia because it is a small state with a population of only 1.4 million. With such a small population, it is exceptionally difficult to be a global leader in several fields.

---

[279] Invest in Estonia, "Estonia leads Europe in startups, unicorns, and investments per capita," Last modified March 2022, https://investinestonia.com/estonia-leads-europe-in-startups-unicorns-and-investments-per-capita/.

[280] EU for Digital, "Azerbaijani officials to visit Estonia for study on cyber security," Last modified May 11, 2019, https://eufordigital.eu/azerbaijani-officials-to-visit-estonia-for-study-visit-on-cyber-security/.

Russian Threat

Estonia faces a unique and persistent threat from Russia that forces cybersecurity to be a national priority. Because of its Soviet past, ethnic Russians make up 25% of Estonia's total population. Additionally, Estonia shares a border with Russian and is only 338 kilometers from Russia's second largest city, St Petersburg. In 2007 Estonia suffered a cyberattack on its critical infrastructure, usually referred to as the "Bronze Night." The attack was prompted by the removal of a Soviet World War II statue in Tallinn. For ethnic Russians living in Estonia the statue was a memorialization of those who died in the war, while for ethnic Estonians the statue was a symbol of bitter occupation. Violent protests broke out in Tallinn between the local police and those who did not want the statue to be removed. The following day, a series of deliberate and targeted denial-of-service (DDoS) attacks against the country began. Government websites, major banks, media organizations, and political parties were affected by the attacks that lasted twenty-two days occurring in several waves. The Russian government was originally blamed for the attacks, strengthened by the fact that political tensions between the two countries had dramatically worsened in the weeks before. However, the Russian governments involvement cannot be properly verified as it impossible to prove who was behind the attacks – most experts believe that politically motivated hackers were responsible.[281] This was a pivotal moment for the entire country and especially for legislators who released the first national cybersecurity later that year. Although the Bronze Night was pivotal, it was only the first of Russian threats that Estonians paid attention to.

Several events involving the Russian government impacted Estonia's cybersecurity strategy following the 2007 attack. The 2008 Georgian-Russian war highlighted Russia's willingness to use cyberattacks against post-Soviet states in the name of protecting Russian citizens abroad. In response to Georgia's attack against separatist forces in South Ossetia, Russia sent

[281] Nick Robinson, and Alex Hardy, "Estonia: from the Bronze Night to cybersecurity pioneers," In *The Routledge Companion to Global Cyber-Security Strategy*, edited by Scott Romaniuk and Mary Manjikian, 211–255. London: Routledge, 2021.

military troops and attacked Georgian institutions with DDoS attacks and defacements. There were two phases of attacks with the first focused on news and government websites and the second focused on financial, business, and education institutions. Six years later, the annexation of Crimea reminded the Estonia government of the Soviet occupation and forced it to think about ensuring the continuity of government and public services in the face of a Russian attack. Consequently, a few years later Estonia made its data embassy agreement with Luxembourg. More recently, Estonia has paid close attention to and strongly detested Russia's invasion of Ukraine. In midst of the conflict, Russian has questioned the sovereignty of Lithuania, another Baltic state. This ongoing conflict will certainly impact the Estonia's next cybersecurity agenda.

Replicability

The heightened sense of cybersecurity that exists in Estonia is the cornerstone of the country's cybersecurity strategy, but it cannot be replicated in other countries, mainly because of the context in which it was developed. As the Internet became more prominent globally, Estonia needed to rebuild its economy and infrastructure. This, combined with the Russian threat, created a situation that put Internet technology and cybersecurity at the forefront of the Estonian government's strategy. Overtime, with policies such as the Tiger Leap Initiative and the relaxation of laws to foster start-up innovation, Internet technology, and cybersecurity, became increasingly important to the Estonian general population as well. In a practical sense, the circumstances that forced Estonia to prioritize e-Governance and cybersecurity are not replicable; this is because the Internet is no longer an emerging technology, it has permeated most of globe and many aspects of daily life. A case could made that a country whose economy and infrastructure needs to be rebuilt could prioritize e-governance and cybersecurity in a similar manner as Estonia in the 1990s. However, the materials required to accomplish that are much more expensive and less accessible to a country in that position. Additionally, without the threat of a cyberattack that could jeopardize sovereignty and wreck an economy, there is no guarantee that cybersecurity would remain a priority. The importance

Estonia places on cybersecurity is therefore essential to understand, and those hoping to learn lessons from Estonia's cybersecurity strategy must know which aspects of that strategy cannot be replicated.

International Cooperation in the EU and NATO

Cyber Deterrence

Estonia's international cooperation in the EU and NATO is essential to its cybersecurity strategy, especially for cyber deterrence. "Deterrence" Nye argues, "can be understood as dissuading someone from doing something by making them believe the costs will exceed the expected benefit."[282] This definition can also apply to the field of cybersecurity. Although some cybersecurity scholars argue that cyber deterrence is not possible, a case study on Estonian cyber deterrence by Pernik, proves that Estonia has been successful in the field.[283] According to Pernik,, Estonia's cyber deterrence policies and practices are built on tools including cyber norms, international cooperation, information sharing with allies, defense, risk management, law enforcement and public attribution.[284] Tools like cyber norms, law enforcement, and risk management are most beneficial in deterring domestic cyber threats, while international cooperation, information sharing with allies, defense, and public attribution are most beneficial in deterring foreign cyber threats. The study also argues that Estonia's success with cyber deterrence is rooted in its layered and whole-of-society approach, where international cooperation and presence is the first layer.

Importantly, Estonia has collective defense through its membership in the EU and NATO. The EU has the power to impose damaging sanctions on individuals, organizations, and states that use cyber-attacks or break

---

[282] Joseph S. Nye, "Deterrence in Cybersecurity." *China US Focus*, June 12, 2019.

[283] Piret Pernik, "Hybrid CoE Paper 8: Cyber deterrence: A case study on Estonia's politics and practice." The European Centre of Excellence for Countering Hybrid Threats. Last modified October 12, 2021. https://www.hybridcoe.fi/publications/hybrid-coe-paper-8-cyber-deterrence-a-case-study-on-estonias-policies-and-practice/.

[284] Ibid.

International cyber laws. Similarly, in 2016, NATO added cyberspace as an operational domain that, when attacked, could trigger collective military defense.[285] The power of these two organizations in the face of a cyber attack has been instrumental in preventing Russian cyber attacks following the Bronze Night.[286] This has not been the case in other post-Soviet countries that do not have such membership.

Replicability

Estonia's cyber deterrence through international cooperation in the EU and NATO has limited replicability, particularly in Europe. Countries such as Ukraine and Georgia, who have expressed interest and have the potential to join those organizations, are good examples.[287] However, cyber deterrence through collective defense could also be possible outside of Europe and North America if there was an organization with advanced cyber defense capabilities. However, those hoping to learn cyber deterrence from Estonia would benefit more from attempting to implement the other tools that Estonia uses for cyber deterrence (namely cyber norms, law enforcement, risk management, and public attribution), which are replicable.

National Cybersecurity Agendas

National cybersecurity agendas with specific and achievable goals are an essential aspect of Estonia's cybersecurity strategy that can be replicated in other countries. Following the 2007 Bronze Night attacks, the Etonian government developed national-level cybersecurity strategies to move the country forward and protect it from increasing threats. So far, three national strategies have been produced, and a fourth is expected in the

---

[285] See https://www.nato.int/cps/en/natohq/topics_110496.htm?selectedLocale=en for more information on cyberspace as the fifth domain of NATO's collective defense.

[286] Kevin Kohler, "Estonia's National Cybersecurity and Cyberdefense Posture" (Zurich: Center for Security Studies (CSS), ETH Zurich, 2020), https://css.ethz.ch/en/publications/risk-and-resilience-reports/details.html?id=/e/s/t/o/estonias_national_cybersecurity_and_cybe.

[287] It is worth noting here that Ukraine and Georgia do share some similarity with Estonia because they are both post-Soviet states who have large Russian minorities and have been attacked by Russia.

coming years. Importantly, the strategies lay out goals based on the past (world events, its historical perspectives), the present (needs of the country), and the future (potential advancements in technology or threats). Additionally, the goals are realistic and achievable.

First National Strategy

The first national cybersecurity strategy was released in 2008 and marked a new era for the country's national security.[288] Estonian cyber defense underwent significant organizational changes to improve coordination and collaboration within the government and between the government and private sector.[289] The primary aim of the first strategy was to reduce the vulnerabilities of cyberspace in the nation as a whole. Among the main goals were establishing a multilevel system of securities measures, expanding Estonia's expertise and awareness of information security, adopting an appropriate regulatory framework to support the security and extensive use of information systems, and consolidating Estonia's position as one of the leading countries in international cybersecurity efforts. Additionally, there were two subgoals that included providing a comprehensive assessment of infrastructure interdependence, cross-dependencies, and development of measures to protect it in the future and committing to cybersecurity education, research, and development. The main legislative outcome included a law that recognized cyberattacks can constitute a national emergency, the re-defining of critical services and coordination agencies, an implementation of mandatory IT security standards, the creation of the Estonian Cyber Defense League, and changes to the penal code covering cybercrime. This strategy lasted until 2013.

---

[288] Estonian Ministry of Defense, Cyber Security Strategy Committee, *Cyber Security Strategy*, 2008, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiyr-in4Mz7AhW0lmoFHeMpA8wQFnoECBIQAQ&url=https%3A%2F%2Fwww.enisa.europa.eu%2Ftopics%2Fnational-cyber-security-strategies%2Fncss-map%2Fstrategies%2Fcyber-security-strategy%2F%40%40download_version%2F993354831bfc4d689c20492459f8a086%2Ffile_en&usg=AOvVaw2__tiWtd_XI9UlAwOg-zGW.

[289] Robinson, 213.

Second National Strategy

The second national cybersecurity strategy was released in 2014[290] with a focus on critical infrastructure, consolidation, and digital continuity. It places a greater emphasis on protecting critical infrastructure and the preservation of vital service sin both public and private sector with two major structural changes.[291] The first structural change brought cybersecurity policy under the control of Ministry of EAC, while the second structural change created a cybersecurity council. This strategy had five strategic objectives: ensuring the protection of information systems underlying important services, enhancing the fight against cybercrime, development of national cyber defense capabilities, managing evolving cybersecurity threats, and implementation of cross-sectoral activities. An important change in language and tone occurred, proposing the use of alternate ICT infrastructure solutions and secure storage of data oversees (data embassy), in the event of a large-scale disruption. Once again, the strategy seeks to develop Estonia's public awareness as a means to combat cybercrime and role as a digital power/cybersecurity leader. This strategy spanned for three years.

Third National Strategy

The third national strategy was released in 2019[292] amidst the Ukrainian border conflict and increasing global cyberattacks. It details Estonia's ability to withstand cyber threats and highlights cybersecurity as a shared responsibility across society. There are no major structural changes introduced, but there are main objectives including the development of a sustainable digital society, cybersecurity research and development,

---

[290] Republic of Estonia, Ministry of Economic Affairs and Communication, *Cyber Security* Strategy, 2014, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf.

[291] Robinson, 216.

[292] Republic of Estonia, Ministry of Economic Affairs and Communications, *Cybersecurity Strategy*, 2019, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwilgv-j78z7AhUeRDABHT2fAIcQFnoECA8QAw&url=https%3A%2F%2Fwww.mkm.ee%2Fmedia%2F703%2Fdownload&usg=AOvVaw0QU1XSmTUWuP8cLmE80cTo.

international cybersecurity contributions, and producing a cyber-literate society.[293] The strategic objective here is to prepare country for the future by making it more resilient. Also worth noting is that the Estonian government acknowledges that its digital ecosystem is susceptible to advancing cryptography and calls for a big picture view that ensures compliance with security standards.

Replicability

Countries hoping to learn from Estonia's cybersecurity strategy should focus on these national agendas. There are several reasons for this. First, the Estonian government publishes these agendas (and so much more) on government websites for everyone to view. There is an abundance of information about these agendas, both from the Estonian government and academics from various countries. Second, the strategies were produced chronologically with evidence of Estonia's existing cybersecurity capabilities available for each strategy. This means countries can look at Estonia's capabilities for each of the strategies and find which strategy most closely matches its own capabilities. Additionally, Estonia's strategies can be compared to other countries' strategies to determine why Estonia has been successful in reaching its goals and theirs have not. Third, the goals in the agendas are specific and achievable, usually resulting in legislation. Countries hoping to develop their own goals in relation to cybersecurity would benefit from looking at these strategies and mimicking their characteristics or methods, even if the goals are different than those in the strategy.

The Estonian Cyber Defense League[294] referenced in the first national cybersecurity strategy is worth exploring in more detail because of its unique and innovative model. The league, existing under the Cyber Defense Unit, uses volunteer involvement in national cyber defense. Its main focus is on "strengthening the professional cyber defense skills of its volunteer

---

[293] Robinson, 218.

[294] See https://ccdcoe.org/library/publications/the-cyber-defence-unit-of-the-estonian-defence-league-legal-policy-and-organisational-analysis/ for more information on the Estonian Cyber Defense League.

members in order to prepare and enhance support capabilities in a crisis."[295] In fact, the Estonian Ministry of Defense requested that NATO do a case study of the league so that other countries may follow a similar model. The case study is meant to explore the legal context of using volunteers and identifies the major issues and concerns with the Estonia's Cyber Defense League. For countries who are not able to afford competitive wages for cybersecurity professionals, this model is a viable option. The Estonian government suggests, "the emergence of a bottom-up initiative to support national defense and security objectives with regard to the emerging security threats from the ICT environment can be regarded as a rather organic development." This is because the Cyber Defense Unit is built on longstanding private-public cybersecurity cooperation and well-established volunteer national defense tradition. Countries hoping to implement a similar model should be cognizant of the context in which Estonia's Cyber Defense Unit was built, as to not develop false expectations.

Conclusion

This paper has discussed three aspects of Estonia's cybersecurity strategy, identifying those aspects that are replicable and those that are not. Heightened perception of cybersecurity's importance, international cooperation, and national agendas were the aspects chosen because they are the core of Estonian cybersecurity. This paper covered Estonia's heightened perception of cybersecurity's importance more thoroughly than the other two aspects because it is the most neglected in literature on Estonia's cybersecurity strategy. Understanding why cybersecurity is so important to Estonians is essential to understanding Estonia's cybersecurity ecosystem as a whole, and therefore enables us to identify which aspects of that system are replicable. International cooperation in the EU and NATO has been essential for Estonia's cyber deterrence, especially from Russian cyber-attacks which have been widespread across the post-Soviet region. Estonia's national cybersecurity agendas are the most replicable aspect of the country's

[295] From "The Cyber Defense Unit of the Estonian Defense League: Legal, Policy, and Organizational Analysis," NATO Cooperative Cyber Defense Centre of Excellence, 2013.

cybersecurity, with methods that can be used in a wide range of countries. For example, countries with smaller economies and less cybersecurity professionals could benefit from an Estonian-style Cyber Defense League. Although this paper has provided an in-depth analysis about three critical aspects of Estonia's cybersecurity ecosystem, there is still much more to explore. The country is eager to provide cybersecurity assistance to other countries and maintain its position as a global leader in the field.

Figure 3: Timeline of e-Governane in Estonia 1991-2005

Year	Event	Challenge	Effect
1991	Resuming independence	To build new technology infrastructure from scratch while catching up with West as quickly as possible.	Policy makers seize a unique opportunity to create low-cost, cutting-edge systems based around accessibility and efficiency.
1994	First draft of the "Principles of Estonian Information Policy"	To solve social challenges stemming from political uncertainty with IT solution.	1% of GPD earmarked as state funding for IT.
1996	Launch of the Tiger Leap Initiative	To catch up to the West by updating local IT infrastructure and establishing computer skills as a priority in schools.	99% if the population uses the internet regularly; Estonia ranked as #1 in the Digital Development Index.
1996	First e-banking services	To make banking solutions available to client in rural communities.	The development of high-quality e-banking services, which encouraged people to get online and embrace e-government, and later, e-ID.
1996	e-Cabinet meeting	To reduce government bureaucracy by making e-solutions part of governance.	The average length of Estonian cabinet meetings shrinks to 30 minutes from five hours.
2000	e-Tax board	To maximize state tax revenue to support the growing needs of a developing society.	To declare taxes now takes about 3 minutes online; 98% of people declare their income online.

Year	Event	Challenge	Effect
2000	m-parking	To manage growing traffic in urban areas, and to create a low-cost parking infrastructure.	95% of parking fees are paid via mobile phones; this solution has been adopted in several countries.
2001	X-Road	To create national integration platform to reduce data exchange costs, and end data leads from existing unsecured databases.	X-road became the backbone of e-Estonia, allows the public and private sector information systems to link; 99% of public services are available online 24/7.
2002	e-ID and digital signature	To securely identify residents using public and private e-services.	98% of Estonians have an ID card; digital signatures save 2% of GPD annually.
2005	i-Voting	To make voting more accessible to a country with a low population density.	1/3 of votes in elections are cast online, with votes cast from over 110 countries.

Source: https://e-estonia.com/story/