Université de Strasbourg

Sciences Po Strasbourg
École
de l'Université de Strasbourg

INSTITUT D'ETUDES POLITIQUES DE STRASBOURG

Université de Strasbourg

How the 2007 Cyber Attacks shaped Estonia's International Role

Margaux Martin

Mémoire de 5ème année, filière « Négociations et Expertises Internationales »

Sous la direction de Monsieur Emmanuel Droit

2020/2021

" L'Université de Strasbourg n'entend donner aucune approbation ou improbation aux opinions émises dans ce mémoire. Ces opinions doivent être considérées comme propres à leur auteur[e] "

To Bree V.d.K. and her determination

Acknowledgments

I would first like to thank my supervisor, Professor Emmanuel Droit, whose expertise was invaluable in formulating the research questions and methodology. His insightful feedback pushed me to sharpen my thinking and brought my work to a higher level.

I'd also want to thank everyone who took the time to share their expertise and opinions with me.

In addition, the completion of my dissertation would not have been possible without the support and nurturing of Georges Kanaan.

Table of Contents

INTRODUCTION

In a 2016 Medium post, Taavet Hinrikus, co-founder and president of Wise, an Estonian remittance firm, wrote: *'Creating a new country from scratch has given Estonia the license to imagine what a country could be.'*[1] This quote exemplifies how Estonia, a small northern European country bordered to the north by the Gulf of Finland, to the west by Sweden, to the south by Latvia, and to the east by Russia, has been able to reclaim possession of its destiny after a long history as a colonized country.

Estonia's past is marked by a succession of dominances until the 1940s[2]. At the end of the eleventh century, the Estes, a Finno-Ugric-speaking community in present-day Estonia, have had to endure Denmark's dominance. The Danes sold the country to the Teutonic knights in 1346. Estonia was annexed by Sweden in 1564. In 1721, it was ceded to Russia under Peter the Great by the Treaty of Nystadt. Russia established the Russian code and declared Russian to be the official language alongside German in 1835. In the late nineteenth century, Russia attempted to incorporate Russian into numerous educational establishments in order to free Estonians from German dominance. Germany, who had coveted Estonia during World War I, eventually took it over in 1918. On February 24, 1918, Estonian independence was declared when German and Russian forces were fighting each other. Following the surrender of the Germans, the Estonian army, supported by the Finnish army and the British navy, concluded the push out of the Red Army. A democratically elected government was created. It was successful in introducing an agrarian reform that called for the resettlement of land taken over by the Baltic barons, but it was never fully functional. Estonia also had a currency, the mark, which was replaced by the crown in 1928, a blue, black and white flag, and a national anthem as early as 1919.

This first period of independence ended in June 1940, when the Soviet Union occupied Estonia. The absorption into the Soviet empire took place on August 6, 1940. During Hitler's troops' offensive toward Russia in 1941, Estonia was once again invaded by the German army. It was later occupied by the Soviet Union in 1944 and became the Estonian Soviet Socialist Republic.

[1] Taavet Hinrikus, 'National borders – a thing of the past?', (2016), https://medium.com/transferwise-ideas/national-borders-a-thing-of-the-past-71cb1cf4ecf9, accessed on May 17th, 2021

[2] Jean-Pierre Minaudier, 'Histoire de l'Estonie', https://www.france-estonie.org/histoire-de-lestonie-3-des-empires-a-leurope-1918-2004/, accessed on May 17th, 2021

This annexation, like that of the other two Baltic states, was never recognized by the international community. From 1985 onwards, Mikhail Gorbachev's agenda of openness, glasnost, reawakened autonomist and then independence claims in Estonian soviets, taking over from street protests calling for democracy. Moscow initially opposed independence, but later recognised it in August 1991. Russian forces remained in Estonia until 1994, but democratic institutions were already in place, as the country drifted closer to NATO and the European Union.

The new constitution of 1992 created a unicameral legislature, the Riigikogu, the parliament, whose members are directly elected by proportional representation for four-year terms in order to preserve the Estonian nation and culture[3]. The Riigikogu elects the President, who is both the head of state and the supreme leader of the armed forces, for a period of maximum two successive five-year terms. The Prime Minister, who is appointed by the President, and the Council of Ministers exercise executive authority. The government is in charge of enforcing domestic and international policy as well as overseeing the work of government agencies[4]. Political life is rather conciliatory, with the majority of parties supporting economic liberalism[5]. Only the Centrist Party, which regularly wins elections but cannot form a government, is marginally less liberal and more concerned with improved ties with Russia. Until 2008, Estonia had no left-wing parties.

Estonia also became a member of the Atlantic Alliance in March 2004 and the European Union in May 2004. Simultaneously, Estonia has had to deal with complicated ties with Russia: a spying scandal erupted in 2000, leading to the removal of ambassadors from both nations[6], and negotiations on the final delineation of the boundary between Russia and Estonia resulted in a treaty in 2005, but it was promptly denounced by the two signatories[7]. Russian-Estonian ties are

[3] Riigi Teataja, 'The Constitution of the Republic of Estonia', (1992), https://www.riigiteataja.ee/en/eli/ee/530102013003/consolide, accessed on May 17th, 2021

[4] EESTI, 'Government of the Republic', https://www.eesti.ee/en/republic-of-estonia/government-of-the-republic/, accessed on May 17th, 2021

[5] Vello Pettai, 'political Parties in Estonia', (2006), https://www.ucis.pitt.edu/nceeer/2003-816-05g-Pettai.pdf, accessed on May 17th, 2021

[6] Jaclyn Sindrich, 'Russian diplomats expelled on spying charges', (2000), https://www.baltictimes.com/news/articles/2493/, accessed on May 17th, 2021

[7] Dmitri Lanko, 'The regional approach in the policy of the Russian Federation towards the Republic of Estonia', (2013), https://www.ssoar.info/ssoar/bitstream/handle/document/36537/ssoar-balticreg-2013-3-lanko_dmitry-The_regional_approach_in_the.pdf?sequence=1&isAllowed=y&lnkname=ssoar-balticreg-2013-3-lanko_dmitry-The_regional_approach_in_the.pdf, accessed on May 17th, 2021

strained further since Estonia is a NATO member and a member of the European Union. As a result, it has explicitly chosen a side.

Estonian demographics have also compromised ties. Prior to World War II, Estonians made up 88.1 percent of the Estonian population. The remainder of the population was made up of Russians (8.2%), Germans (1.5%), Latvians, and Jews[8]. During the Second World War, many minorities fled Estonia, and at the end of the war, Estonians made up 97 percent of the population. During the Soviet era, there was a massive influx of people from the Soviet Union. Estonians decreased from 88 percent in 1934 to 61.5 percent in 1989. In 2010, Estonians made up 68 percent of the population, while Russians made up 25%, Ukrainians made up 2%, Belarusians made up 1%, and Finns made up 1%[9].

The topic of incorporating Russian speakers is a source of consternation. Minorities are protected by a law passed in 1925, which requires them to establish independent cultural administrations. They are not, however, immediately given citizenship; they must demonstrate their ability to integrate. The original scheme, implemented in 1995, was as follows: descendants of Estonian citizens from 1939, regardless of language, were qualified for citizenship; however, those who entered or were born on Estonian territory after 1944 had to pass a language examination as well as another on culture, organizations, and national symbols. They could apply for Russian citizenship if they failed or declined. Following criticism from Russia and the EU, this scheme was relaxed in 1998[10].

Inter-ethnic relations are stable, but the two groups do not get along: Estonians continue to behave as though Russian speakers do not exist, and not all Russian speakers have abandoned their colonial disdain for Estonian. This issue taints ties with Russia, which has defended Russian speakers in the Baltic states, screamed discrimination, and even made particularly violent remarks against Estonians[11]. Because of its history, Estonia has a high proportion of Russian speakers in its population, which had an impact during the relocation of the Bronze Soldier in Estonia.

[8] ESA, 'Population of Estonia by population censuses', (1996)

[9] Estonica, 'Composition of the population', http://www.estonica.org/en/Society/Population/Composition_of_the_population/, accessed on May 17th, 2021

[10] Legal Information Centre for Human Rights, 'Minority Rights in Estonia', (2009), https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/EST/INT_CCPR_NGO_EST_99_8742_E.pdf, accessed on May 17th, 2021

[11] Raivo Vetik, 'Ethnic conflict and accommodation in post-communist Estonia', (1993), https://www.jstor.org/stable/424806?seq=1, accessed on May 17th, 2021

Shortly after achieving independence from the former Soviet Union, the Estonian government was prompt to establish a new e-society: in the 1990s, Estonia initiated its first digital policy initiatives and established an Information Authority, which was in charge of information security[12]. Furthermore, Estonia has reinvented the concept of the State as a network of resources that places the user at the forefront and where access to the Internet is a right that any citizen must be granted. As a result, 99 percent of public facilities are now available online through an e-governance scheme. X-Road refers to the digital infrastructure that facilitates digitalization[13]. It serves as the foundation of the e-government system, which manages nearly 2000 services. M-Parking, e-Tax, digital signature, electronic polling, e-Police, and e-Prescription are a few examples. More than 900 interconnected organizations share databases on the state blockchain through an Application Programming Interface, which enables administrations to connect and exchange decentralized data[14]. Any Estonian citizen can connect to an online portal using their electronic identification card to access a variety of resources, such as declaring taxes, opening a bank account, registering a vehicle, forming a business, and so on. Furthermore, online voting has been a reality for Estonians since 2005[15]. With such ease of access and speed of public services, it's easy to see how the Internet has become a sign of independence and democracy in this post-Soviet country. The specialized magazine Wired called it *'the most advanced digital society in the world,'*[16] but what forced the government to go this route was a shortage of resources, especially to ensure the proper functioning of the public administration. Efficient public services are not cheap.

As a result, Estonia has emerged as a blueprint for the use of emerging technologies to increase government performance, ease citizens' lives, and strengthen the economy. Nonetheless,

[12] Elena Bajric, 'Portrait de l'Estonie, la société digitale par excellence', (2020), https://www.eyes-on-europe.eu/estonie-la-societe-digitale-par-excellence/, accessed on May 17th, 2021

[13] Wen Hoe, 'E-stonia: One small country's digital government is having a big impact', (2017), https://www.innovations.harvard.edu/blog/estonia-one-small-country-digital-government-having-big-impact-x-road, accessed on May 17th, 2021

[14] European Commission, 'Case Study Report e-Estonia', (2018), https://jiip.eu/mop/wp/wp-content/uploads/2018/10/EE_e-Estonia_Castanos.pdf, accessed on May 17th, 2021

[15] Perrine Signoret, 'Nouvelles technologies: pourquoi l'Estonie a dix ans d'avance sur les autres pays', (2017), https://lexpansion.lexpress.fr/high-tech/nouvelles-technologies-pourquoi-l-estonie-a-dix-ans-d-avance-sur-les-autres-pays_1945700.html, accessed on May 17th, 2021

[16] Matt Reynolds, 'Welcome to E-stonia, the world's most digitally advanced society', (2016), https://www.wired.co.uk/article/digital-estonia, accessed on May 17th, 2021

as with the various ethnic groups in Estonia, this very beneficial trait would prove to be a source of instability during the 2007 attacks.

In this paper, we will examine Estonia's position in cyberspace following the 2007 cyberattacks. First and foremost, we must define the main terms. Cyberspace refers to both the Internet and the 'space' it creates, i.e., an intangible space in which de-territorialized exchanges between inhabitants of all nations occur instantaneously, obviating the concept of time. In *La Géopolitique pour Comprendre le Cyberespace*, Frédérick Douzet[17] takes a very visual approach, stating that cyberspace is made up of four superimposed layers that interact with one another. The physical layer is the first. The physical architecture of the Internet is made up of submarine and terrestrial cables, radio relays, and computers: a collection of materials placed on the ground that can be constructed, changed, or removed, as well as attached or disconnected from the network. The second layer is the logical infrastructure. It contains all of the facilities that allow data transfer between two points on the network and, as a result, allow information travel from its source to its receiver, broken down into small data packets. The logical architecture is based on an important standardisation, a shared language that enables all computers in the world to communicate with each other, the Internet Protocol (TCP/IP). The third layer is made up of software, which are computer programs that enable people to access the Internet without having much knowledge of computer programming (e-mail, social networks, search engines, etc.). Finally, the fourth layer, which is often referred to as semantic, is that of knowledge and social contact. It is the layer of consumers, conversations, and interactions that occur in real time around the world. As a result, cyberspace is a digital world created by machines and computer networks in which humans and computers coexist and which encompasses all forms of online interaction. Cyberspace has also sparked strategic interest because it provides a new arena for the exercise of power and dominance.

Threats exist in cyberspace, just as they can in any other strategic space (air, sea, etc.). A cyber-attack, also known as a malware attack, is a voluntary and destructive activity carried out via a computer network with the intent of causing harm to information and the individuals who

[17] Frédérick Douzet, ‘Understanding cyberspace with geopolitics’, (2014), https://www.cairn-int.info/article-E_HER_152_0003--understanding-cyberspace-with-geopolitic.htm, accessed on April 29th, 2021

process it[18]. A cyber-attack can be carried out by a single person, a group of hackers, a government, or a criminal enterprise. Cyber threats are aided by the growing volume of information made accessible online through the cloud[19], as well as device security vulnerabilities. A cyber-attack is therefore the malicious use of cyberspace to interrupt, disable, or monitor an IT infrastructure, as well as to destroy data integrity or steal information.

In this paper, I will look at how Estonia's international role has shifted in the aftermath of the 2007 cyber-attacks, and how the country has been able to carve out a new reputation as a cyber norm-entrepreneur. I will also assess Estonia's ability to fully position itself as a world leader in cyber security. To ensure a rigorous and accurate study of this subject, which is poorly documented due to its strategic nature and is not covered much in the university curriculum, I conducted a series of interviews in order to confront the empirical data from my research with the everyday reality of people in the field of cyber security. These interviews are used throughout the analysis. In parallel, the Covid 19 pandemic allowed me to follow many webinars about cyberspace and Estonia's role on the international scene.

In the first section, we will address the 2007 Estonian attacks, their effect on Estonian society, and the reactions and repercussions that resulted. Then, we'll look at how these attacks allowed Estonia to carve out a new presence on the international stage, and how major international organisations were able to profit from this new expertise and skills when assisting Estonia. Finally, we will look at the constraints that the country faces in establishing cyber norms.

[18] Louis Gautier, 'Cyber : les enjeux pour la défense et la sécurité des Français', (2018), https://www.cairn.info/revue-politique-etrangere-2018-2-page-29.htm, accessed on May 17th, 2021

[19] **Glossary**

PART 1: The 2007 cyber-attacks and the implications for the Estonian society

This part will go into further detail on the cyberattacks that occurred in Estonia in the spring of 2007, examining the key causes as well as the vulnerabilities that existed within the country. We will then examine the responses of Estonian authorities as well as that of the general public, before turning our attention to reactions outside of Estonia, notably in the United States, Russia, and the European Union. We shall end this part by discussing the many ramifications for Estonians and the condemnation of those responsible.

Chapter 1: Understanding the 2007 cyber-attacks

In April and May 2007, Estonia became the target of the *'world's first cyber-attacks against a nation state'*[20]. The media largely labelled the events as a *'cyber war'*[21] and the Estonian president stated that this was the *'Web War One'*[22]. This chapter considers the 2007 cyber-attacks, the trigger element and their nature and effects.

A) The course of events: trigger element and background

i. *The Bronze Soldier Statue*

The cyber-attacks against Estonia took place in response to the announcement of the Estonian Government on January 10th, 2007, to relocate a Soviet-era war memorial statue, the Bronze Soldier. The statue was ultimately moved from a park in the Tallinn district of Tonismagi to the Defense Forces Cemetery, 2 kilometers southeast from its initial position. It was the decision to relocate the statue that sparked the cyber-attacks. As mentioned earlier, there are ethnic tensions

[20] '*On April 27, Estonia became the unprecedented victim of the world's first cyber-attacks against a nation state*', Jeff Goldstein, 'Estonia's Cyber Attacks: Lessons Learned' (Wikileaks Cable, 6 June 2007), https://wikileaks.org/plusd/cables/07TALLINN375_a.html, accessed March 15th, 2021

[21] Ian Traynor, 'Russia accused of unleashing cyberwar to disable Estonia', The Guardian (17 May 2007), https://www.theguardian.com/world/2007/may/17/topstories3.russia, accessed March 15th, 2021

[22] Toomas H Ilves, 'Address by the President of Estonia' (speech at the 67th session of the United Nations General Assembly, New York, 26 September 2012), https://vp2006-2016.president.ee/en/official-duties/speeches/7991-address-by-h-e-toomas-hendrik-ilves-president-of-estonia-to-the-67th-session-of-the-united-nations-general-assembly-un-headquarters-new-york-september-2012/, accessed March 15th, 2021

in Estonia and the relocation of the statue caused great anger among Estonia's ethnic Russians and their advocates in Russia[23]. For them, the statue was a commemorative monument to the Soviet soldiers who died fighting for the Soviet Union during the Second World war. However, for the Estonians it was a constant reminder of their oppression under the Soviets[24]. Preparations for the statue's removal on April 26th went along with disagreement and protests, which led to violence and demonstrations in the streets of Tallinn. The disruptors were mostly Estonians of Russian descents, they represent a quarter of Estonia's population[25].

Due to the violent events of April 26th, the Estonian government decided to relocate the statue the following day, before the scheduled date. Protests were also held in Russia. The Estonian embassy was barricaded, and the ambassador assaulted[26]. In addition to the physical demonstrations, discontent was echoed online. Following the relocation and protests, there were several waves of cyber-attacks in Estonia, targeting a large number of Estonian websites including the president's, prime minister's, parliament's, most government departments, political parties, media organizations and banks[27].

ii. Estonian e-government

The second part of the twentieth century was challenging for Estonia. It was able to break free from Soviet reliance, but it was impoverished. It swiftly modernized, skipping a generation of innovation. Estonians, for example, are not accustomed to utilizing faxes or checks[28]. Unfortunately for Estonia, the state had been integrating the use of the Internet into public life, so it was particularly vulnerable to cyber-attacks. For instance, voting and filling of taxes were

[23] ICDS, 'Russia involvement in the Tallin Disturbances', https://icds.ee/en/russias-involvement-in-the-tallinn-disturbances/, accessed March 15th, 2021

[24] Francis Tapon, 'The Bronze Soldier explains why Estonia prepares for a Russian cyberattack', Forbes (7 July 2018), https://www.forbes.com/sites/francistapon/2018/07/07/the-bronze-soldier-statue-in-tallinn-estonia-give-baltic-headaches/, accessed March 15th, 2021

[25] Isabelle de Pommereau, 'Estonia reaches out its ethnic Russians at long last', DW (24 February 2018), https://www.dw.com/en/estonia-reaches-out-to-its-ethnic-russians-at-long-last/a-42680725, accessed March 15th, 2021

[26] Ian Traynor, 'EU Protests over Russians Attacks on Ambassadors', The Guardian (3 May 2007), https://www.theguardian.com/world/2007/may/03/russia.eu, accessed March 15th, 2021

[27] Rain Ottis, 'Analysis of the 2007 Cyber-attacks against Estonia from the information warfare perspective', https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf, accessed March 15th, 2021

[28] Interview with Professor Rain Ottis

already available online, communications between the state and the citizens and storage of public records took place over the Internet. The Estonian parliament, Rigiikogu, had also enacted that access to the internet was a human right in February 2000. Because the use of internet was heavily embedded into public life in 2007, Estonia was considered a particularly well wired country, even when compared to the average European criteria[29]. The establishment of Estonia's online government services started in the 1990s as part of the program 'Tiigrihüpe', in English, Tiger Leap'[30]. It aims to invest in development and expansion of computer and network infrastructure in Estonia, with a particular emphasis on education. It resulted in the creation of an electronic state, an 'e-state'. This process also involved efforts by the government to accelerate access to the Internet through free Internet stations. A digital national population registry system was also created to store citizen's information digitally. In parallel, a state information system was developed to build a common service space that allowed the Estonian state to function in cyberspace[31]. Estonia had also introduced electronic identification cards in 2002. These cards were associated to each citizen's personal information in government databases and allowed users to file taxes, access social security benefits and other services[32]. The state portal provided a centralized online platform through which these services could all be accessed, a unique infrastructure at the time. Consequently, by 2007 Estonia was an innovative state in terms of e-government and integration of the Internet into its nation's everyday life. Nevertheless, the 2007 cyber-attacks showed that technological advancement could also be a vulnerability, giving new opportunities to attack the e-state in cyberspace.

[29] Joshua Davis, 'Hackers take down the most wired country in Europe', Wired (21 August 2007), https://www.wired.com/2007/08/ff-estonia/, accessed on March 15th, 2021

[30] Saarenmaa Kaisa, 'The Tiger Leap – Information society in Estonian frames' (Autumn 2002), https://longterm.softf1.com/2018/blog_resources/2002_xx_xx_The_Tiger_Leap_Information_Society_in_Estonian_Frames_by_Kaisa_Saarenmaa_and_Osma_Suominen_keywords_history_education_Internet_network_computers.pdf, accessed on March 15th, 2021

[31] Republic of Estonia Information System Authority, 'State information system in Estonia' (2007), https://www.ria.ee, accessed on March 16th, 2021

[32] Ibid.

B) Progress, nature, and effects of the spring attacks

i. Weeks of coordinated cyber-attacks

Beginning in late April 2007 lasting until the latter half of May 2007, and as a result of the relocation of the Bronze Soldier and the protests that followed, Estonia was victim of cyber-attacks that varied in intensity and complexity. Some reports mention that the first attack occurred late on April 26th, just before the removal of the statue[33] while other sources believe that the attack began in the early morning on April 27th[34]. Both sources agree that the first attack targeted the Minister of Foreign Affairs' website and was followed by attacks against a broad range of government websites. The day after, numerous websites, including the prime minister's, parliament's, government's, and Ministry of Foreign Affairs, had been attacked and rendered inaccessible to users. The attacks that occurred between April 26th and April 29th are regarded as the technologically less sophisticated stage of the attacks. They made use of simple techniques compared with the more complex attacks that started to take place on April 30[35].

Between May 1st and 8th May, the cyber-attacks carried on sporadically. On May 2nd, one of Estonia's newspaper was forced to interrupt international access to its website due to the cyber-attacks[36] which created a huge volume of traffic. On May 9th, there was an impressive number attacks. Estonia was pounded with traffic with over 4 million packets per second, a 200-fold increase[37]. This date was not chosen randomly, it represents an important date in Russia since it is the day, the Soviet Union defeated Germany during the Second World war[38]. The attacks started at midnight Moscow time and they were the strongest and longest attacks of all the previous ones[39]. A large botnet[40], a 'robot network' was used to execute this wave of attacks. Between May 9th and

[33] Gadi Evron, 'Battling Botnets and Online Mobs: Estonia's Defense Efforts During the internet War' (2008), Georgetown Journal of International Affairs

[34] Ibid 8.

[35] Peter Finn, 'Cyber Assaults on Estonia Typify a New Battle Tactic', Washington Post (19 May 2007), https://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html, accessed March 16th, 2021

[36] Ibid 9.

[37] Ibid. 28

[38] Emily Tamkin, '10 Years after the landmark attack on Estonia is the world better prepared for Cyber threats?', Foreign Policy (27 April 2017), https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/, accessed March 16th, 2021

[39] Jose Nazario, 'Estonian DDoS Attacks – A Summary to Date' (17 May 2007), https://www.netscout.com/arbor-ddos, accessed March 16th, 2021

[40] **Glossary**

18th, government websites continued to be subject of attacks as well as Estonian banks. One bank even had to interrupt its online services for several hours[41]. Indeed, Hansabank's customers no longer had access to their accounts via the Internet, a service used by 97% of them. Moreover, the transaction verification system was out of order, which severely disrupted the operation of ATMs and blocked connections with banks abroad. Institutional services were blocked for many and the telecom infrastructure itself was affected. The last considerable cyber-attack took place on May 18th and they abruptly and simultaneously stopped on May 19th, but the banks continued to be attacked, albeit less significantly, after this date.

One thing to highlight in these spring cyber-attacks in Estonia is that a large number of Estonian websites came under attack, but the critical information infrastructure of transportation and energy systems was not targeted.

ii. Different types of attacks and intensities

The 2007 attacks were mainly composed of two waves. The attacks that took place right after the demonstrations in the streets used relatively simple methods compared to the more advanced attacks that started to occur on April 30th. The first wave involved ping flood, which is a common Denial-of-Service (DoS) attack[42]. This type of attack consists of flooding the victim's network with request packets, knowing that the network will respond with an equal number of reply packets[43]. Therefore, it creates a Denial-of-Service because users can no longer access the dysfunctional or even shut down network. This first phase also consisted of malformed web queries allowing for some websites to be hacked or vandalized. Case in point, an apology in Russian was published on the website of the prime minister's political party[44]. The methods used in the first phase of the attacks were therefore objectively simpler than those used later in the second phase.

The more advanced and sophisticated attacks that started to emerge on April 30th were Distributed Denial-of-Service (DDoS) attacks. This kind of attacks consists of multiple computers simultaneously targeting one system[45]. This is achieved through the use of botnets. A bot is a

[41] Samuli Haataja, 'Cyber-attacks and international law on the use of force', chapter 5 'The 2007 cyberattacks against Estonia' (2018)

[42] **Glossary**

[43] **Glossary**

[44] Ibid 20.

[45] Ibid 18.

program created to execute specific actions when it receives a given command. What is interesting is that they can run in the background of compromised computers, waiting for their controllers[46]. Using malicious software like Trojan horses (infected emails and attachments…) can enable cyber criminals to compromise the computer of legitimate users and plant a bot without raising their awareness[47]. A botnet is a network of synchronized bots executing the commands of their controllers. In the Estonian attacks, hundreds of thousands of compromised computers located across 178 counties including Vietnam, Egypt and the United States were involved. There was as many as 1-2 million pre-infected 'bots' ready to launch a coordinated attack to flood websites with data[48]. The objective of the DDoS attacks was to take advantage of the collective strength of the botnets and expose the Estonian websites to much larger volume of data than they can handle, causing them to overload and become inaccessible to users. The attacks were either less than 10 megabits per second (Mbps) or between 10 Mbps and 30 Mbps and lasted less than an hour. Nevertheless, some of the attacks contained much more data, lasting more than 10 hours and reaching over 90 Mbps[49]. These large attacks were sufficient to weaken the Estonian websites due to the low amount of bandwidth available to them. The attacks over 90 Mbps were significant and the biggest one occurred on May 9th. Moreover, the attacks were dynamic and changing in response to countermeasures[50]. While a number of different methods of DDoS attacks were used, the general goal remained the same during the whole wave: it was to prevent legitimate users from using the targeted websites and the services they provided. Finally, the second wave was more sophisticated because DDoS uses multiple internet connections to put the victim's computer network offline whereas DoS only uses a single connection. DDoS are more challenging to identify because they are launched from multiple locations so that the victim can't identify the source of the attack. This is what happened during the spring attacks. Another key element is the volume of data directed towards each target; DDoS enables attackers to send massive volumes of traffic to the targeted network[51].

[46] Stephen Herzog, 'Revisiting the Estonian Cyber Attacks: Digital threats and Multinational Responses', Journal of Strategic Security (Summer 2011)
[47] **Glossary**
[48] NATO CCDCOE, '2007 cyberattacks on Estonia'
[49] Ibid 19.
[50] Ibid 27.
[51] Tim Keary, 'DoS vs DDoS Attacks: The Differences and How To Prevent Them' (9 July 2020), https://www.comparitech.com/net-admin/dos-vs-ddos-attacks-differences-prevention/, accessed March 16th 2021

In both phases, the largest part of malicious network traffic was of Russian-language origin and had indicators of political inspiration[52] but the origin of the attacks was very unclear since they were apparently carried out independently by individuals using their own resources. Therefore, any state sponsor responsible for setting up the attacks was able to act under cover and oppose any accusations.

iii. The lack of information

The DDoS attacks were intended to disrupt the operations of targeted computers and websites as well as the services they provided access to. Some argue that although the economic effects of the attacks are difficult to assess, both the public and private sectors were dependent on Information and Communication Technologies and digital communications. Therefore, the day-to-day operations of the banks, small businesses and government departments were severely compromised. With this in mind, the economic impact could amount from US$27.5 to US$40.5 million[53]. The wider societal effect emanated from the lack of access to information. In fact, because department websites and the usual means and forms of communication between the citizens and the government were temporarily disrupted, it was more difficult to access any type of information and data pertaining to government services. Besides, since the attacks targeted the state portal, they made it easier for people to notice the effects of the attacks and, since the media websites were among the first to come under attack, Estonia could not rely on the usual means of broadcasting information to the rest of the world. These attacks also revealed Estonia's vulnerabilities and showed the potential of cyber-attacks to generate far more lasting destructions than expected. Finally, this event is widely regarded as the first major act of cyber warfare in the world.

[52] Ibid 27.

[53] Sheng Li, 'When does Internet Denial Trigger the Right of Armed Self-Defense?' (2013), Yale Journal of International Law

Chapter 2: Internal and external reactions after the cyber-attacks against Estonia

Following the disclosure of the cyber-attacks on Estonia, reactions were swift, whether nationally in Estonia and through the leaders' accusatory speeches, or internationally, inside the Atlantic Alliance, the European Union, and particularly in Russia, the major nation accused of being behind the operations.

A) Reactions within the country

i. Estonian political class

From the beginning, the government has been open and honest with the public. It might instead have discussed ‘technological issues’, but it used the phrase ‘cyber-attacks’[54]. Because of this transparency, Estonia was able to keep up with digitization and gain the attention of the whole world. For instance, when the computer-based attacks began, the Estonian defense set up a crisis cell to handle the defense. The Estonian authorities also called for international solidarity and the crisis cell received assistance from foreign nations such as Germany, Italy, and Spain, as well as numerous adjacent Baltic nations such as Lithuania and Latvia. It was also aided by foreign internet providers who were ready to shut off connectivity to the most aggressive machines passing via their networks. Above all, after three weeks of assaults and confusion, the Estonian government decided to limit international connections, effectively disconnecting Estonia from the Internet while reducing the number of attacks sufficiently to respond and restore the network[55]. For a few days during the peak of the attacks, Internet access was thus restricted to the outside world. It was a last-ditch effort to keep Internet services running in Estonia.

Moreover, the authorities' language was consistent and geared at reaffirming that moving back the Bronze Soldier Monument was not on the agenda since its relocation was meant to promote societal unity. Furthermore, the goal was to bind Estonia's fate to that of the European Union by claiming that cyber-attacks constitute a flagrant attack not just on Estonia's sovereignty,

[54] Interview with Visiting Fellow at Canadian International Council Josh Gold, June 7th, 2021

[55] Olivier Ricou, ‘chapitre 7, la cyberguerre’, http://www.ricou.eu.org/e-geopolitique/internet_chap8.pdf, accessed on May 27th, 2021

but also on the whole European Union[56]. It was also intended to highlight the Russian government's indirect role. For instance, foreign Minister Urmas Paet stated in May 2007 that the attacks on the Internet pages of Estonian government agencies and the President's office originated from computers and specific individuals of Russian government agencies, including the administration of the Russian Federation's President[57]. Prime Minister Andrus Ansip accused Russia indirectly the day after, saying:

> *'A physical attack against the Ambassador of Estonia to Moscow [...], together with the continuing cyber-attacks from the servers of Russian state authorities, together with tearing the Estonian flag off our embassy and together with statements made by the delegates of the Russian Duma, calling for the change of government in Estonia, indicates that our sovereign state is under a heavy attack. All these events evidence that these are not our internal matters we are dealing with, but it is a well-coordinated and flagrant intervention with the internal affairs of Estonia.'*[58]

Finally, the authorities' language was to demonstrate that Estonia, as one of the most technologically sophisticated countries in the world, was able to effectively fight cyberattacks. As such the country was prepared to face the worst-case scenario[59]. The rhetoric concluded with a request for national and international legislation to be adapted and expanded to deal with emerging dangers such as cyber assaults.

Furthermore, as the first nation to be the target of state-sponsored cyber warfare, Estonia wanted to enlist both the European Union and the Atlantic Alliance in its dispute with Russia, and this request was accepted. Following Estonian President Toomas Hendrik's request for assistance from NATO Secretary General Jaap de Hoop Scheffer, a NATO expert was dispatched to Estonia to assess the situation, and NATO's technical center for responding to such cyber threats, NATO Computer Incident Response Capability, monitored the progress of these cyber-attacks in real

[56] Ibid. 28

[57] Declaration of the Minister of Foreign Affairs of the Republic of Estonia, (May 2007), https://www.valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia, accessed on June 4th, 2021

[58] Prime Minister Andrus Ansip's speech in Riigikogu, (May 2007), https://www.valitsus.ee/en/news/prime-minister-andrus-ansips-speech-riigikogu, accessed on June 4th, 2021

[59] Interview with EU CyberNet Director, Siim Alatalu

time[60]. The Estonians requested two things from NATO. One was political solidarity, which they obtained. Second, was technical aid which they also received that.

Finally, the Estonian Computer Emergency Response Team (CERT) also contacted other CERTs, who, in collaboration with international informal information security networks, assisted in neutralizing widespread denial of service assaults. Simultaneously, Estonian information security professionals neutralized the assaults for three weeks, 24 hours a day, seven days a week, to allow Internet services to operate in Estonia[61]. As a result, Estonian reactions focused on blaming Russia while requesting international assistance and declaring that everything was under control.

ii. The Estonian population and the media

Many Estonians were banned access to standard websites, web-based services, including the opportunity to email legislators. Businesses suffered immediate and opportunity expenses due to their inability to access their funds, move or receive money, and generally do business. However, over half (49%) of Estonians responded in a study that the cyber assaults had little effect on them.[62] Many Estonians were unaware of the attacks and were more concerned about street riots between different the Russian speaking minority and the Estonians[63]. Although many individuals were clearly annoyed by the disruption created by the attacks, they did not target their rage at the state and its incapacity to safeguard its inhabitants and economy from outside intervention. In fact, polls revealed that trust in the administration grew following the riots, from 53 per cent in 2006 to 66 per cent in 2007[64]. The intermediate and long-term consequences concerned national resilience, but the short-term consequences were virtually negligible. Except the fact that protests over the transfer of the war memorial likely exacerbated sentiments and biases between Estonians of non-Russian and Russian descent. The arrest of an Estonian of Russian ancestry in connection with

[60] Laurent Zecchini, 'Les cyberattaques massives d'origine russe contre l'Estonie préoccupent l'Alliance atlantique', (May 2007), https://www.lemonde.fr/europe/article/2007/05/19/les-cyberattaques-massives-d-origine-russe-contre-l-estonie-preoccupent-l-alliance-atlantique_912244_3214.html, accessed on June 4th, 2021

[61] Heli Tiirmaa-Klaar, 'Cyber Security Threats and Responses at Global, Nation-State, Industry and Individual Levels', https://www.sciencespo.fr/ceri/sites/sciencespo.fr.ceri/files/art_htk.pdf, accessed on June 4th, 2021

[62] Cyrus Farivar, 'A Brief Examination of Media Coverage of Cyberattacks (2007 - Present)', https://ccdcoe.org/uploads/2018/10/13_FARIVAR-Web-War-One.pdf, accessed on June 4th, 2021

[63] Interview with Visiting Fellow at Canadian International Council Josh Gold, June 7th, 2021

[64] Ibid. 58

the cyber-attacks added to the situation. According to an opinion survey, 82% of ethnic Estonians agreed with Prime Minister Ansip's handling of the Bronze Soldier relocation, while 84% of the Russian-speaking minority disagreed[65]. However, the cyber-attacks did not result in any public pressure to change the decision to relocate the Tallinn monument. As a result, Estonians were resilient in the face of the attacks while remaining conciliatory toward the government.

The cyber-attack, which targeted media and several other websites, hindered Estonians from accessing information in the manner to which they were used. The attack measures aimed the smooth character of Estonia's digitally dependent state by stopping or rendering less trustworthy and rapid access to information. However, there seemed to have been no attacks on traditional media systems like as television services, implying that the digital shutdown of information was not absolute, even though the platforms that were attacked were sometimes totally unavailable. Otherwise, when the sources of information were available, they conveyed the same information as the Estonian political elite and blamed Russia for the attacks.

B) Reactions outside of Estonia

i. The United States and NATO

The cyber-attacks on Estonia served as a major wake-up call for the United States. Despite the fact that the attacks had no direct impact on the United States, they obviously demonstrated aggressive intent to gain an advantage over cyberspace. Moreover, Estonia is a staunch US ally and is regarded as one of Europe's most pro-US countries. Strong US-Estonia relations have a long history. The United States never acknowledged the Soviet Union's forced absorption of its territory in 1940, and therefore hailed its restoration of independence in 1991. American engagement in Estonia has mostly been centered on strategic partnership and protection support to discourage future Russian aggression and fight threats such as misinformation operations and cyberattacks. Estonia is also a strong and trustworthy transatlantic partner in promoting peace, stability, and democracy in Europe and beyond. It is thus an important American political relay in eastern Europe. Therefore, it has become a crucial ally in the North Atlantic Treaty Organization and for the United States, which is why the United States, and the Alliance did not remain silent following the 2007 attacks.

[65] Ibid. 58

The alliance immediately offered technical support to Estonia and has openly shown its political sympathy with the country. Additionally, cyber-attacks have been identified as a major security concern. While the provenance of these strikes was exceedingly intricate and difficult, NATO spokesperson at the time, James Appathurai, indirectly implicated the Russians, stating:

> *'So, I can't comment about the origin of these attacks, but the Estonians have obviously talked at length about the origin of these attacks.'*[66]

As a result, NATO has sided with Estonia. Secretary General Jaap de Hoop Scheffer, for his part, insisted that the cyberattacks on Estonia had a security aspect and so decided to deploy NATO's specialists to the field to examine what could and should be done. Thus, the alliance's support had two components: the first was political unity, and the second was technical aid. However, NATO never suggested using Article 5 on collective defense, which states that an attack on one ally is deemed an attack against all Allies.

The United States, as well as NATO, respond to the assault by giving cyber security assistance to Estonia. Furthermore, the United States wrote a report on what worked and what failed during the assaults in order to better prepare for future assaults by learning from them[67]. According to the analysis, Estonia was able to respond rapidly to cyber threats due to its modest size. Furthermore, as a result of e-voting, the e-voting security team was quickly seconded to CERT and became a valuable tool in reacting to assaults. On the other hand, Estonia's formal and institutional mechanisms for responding to cyber threats were entirely ineffective, and there was no policy consistency within ministries. The United States helped Estonia, but they also used the attacks as a learning experience.

ii. The European Union

Because Estonia is a member of the European Union, the latter was obligated to respond formally to the attacks sustained by the former. First and foremost, on May 2nd, 2007, the European Union

[66] NATO, 'Press briefing by NATO Spokesman, James Appathurai', (May 2007), https://www.nato.int/cps/en/natohq/opinions_8313.htm?selectedLocale=en, accessed on June 3rd, 2021
[67] Wikileaks, 'Estonia's Cyber Attacks: lessons learned', (June 2007), https://wikileaks.org/plusd/cables/07TALLINN375_a.html, accessed on June 3rd, 2021

demanded Russia to lift the blockade on Estonia's embassy. It asked Russia to uphold its international commitments to embassies and their personnel, and it expressed alarm over the rising violence outside the Estonian embassy in Moscow. At the national level, Chancellor Angela Merkel called Estonian Prime Minister Andrus Ansip to tell him that Germany was doing everything possible to resolve the dispute with Russia[68].

The European Parliament subsequently adopted a resolution on Estonia on May 24th, 2007. In the resolution, it affirms its support and solidarity with Estonia's democratically elected government in its efforts to preserve order, stability, and the rule of law for all Estonians. It also regards the assault on one of the smallest EU member states as a test of European Union unity, and it regards the many attempts by Russian authorities to meddle in Estonia's domestic affairs as unacceptable. The European Union continues by expressing its concerns about the Russian authorities' inadequate protection of the Estonian Embassy in Moscow, as well as the physical attacks on the Estonian Ambassador by 'Nashi' demonstrators[69] and reminds the Russian authorities that the Russian authorities' open and unqualified hostile rhetoric against Estonia is completely incompatible with the principles of international affairs. It finished by highlighting President Toomas Hendrik Ilves' remarks, emphasizing the importance of those who settled in Estonia during the Soviet era and today live in the Republic of Estonia[70]. In addition, the European Union formed working groups to develop a general policy to fight cybercrime in May 2007.

As a result, following the 2007 attacks, the European Union backed Estonians while condemning Russian authorities. However, it had not imposed any sanctions on Russia since no investigation could definitively identify its responsibility. Therefore, the European reaction was more declarations than actions.

iii. Russia

Russia is a key actor in the 2007 attacks since Estonia quickly accused it of being responsible because the Russian authorities contended that the Estonian government's decision to relocate the

[68] Deutsche Welle, 'EU Urges Russia to End Estonia Embassy Blockade ', (May 2007), https://www.dw.com/en/eu-urges-russia-to-end-estonia-embassy-blockade/a-2464370, accessed on June 1st, 2021

[69] Pro-Kremlin youth group

[70] European Parliament, 'European Parliament resolution of 24 May 2007 on Estonia', (May 2007), https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0215+0+DOC+XML+V0//FR, accessed on June 1st, 2021

Bronze Soldier memorial was disrespectful and sacrilegious, and that it will have major ramifications for bilateral relations[71]. However, Russia has disputed the allegations of Estonian authorities from the outset and continues to do so. They further alleged that the Russian government did not organize the cyber-attacks, and that 'patriotic' Russian organisations and people were part in the cyber strikes independently of the Russian government.

Moreover, in opposition to Estonia's intentions, Sergei Ivanov, the First Deputy Prime Minister, called for Russians to boycott Estonian goods and services on April 3rd, 2007, urging *‘Don't buy Estonian items, don't go to Estonia for vacations, go to Kaliningrad’*[72]. Ivanov's call is noteworthy because it demonstrates how little wiggle space the Kremlin has in its fight with Estonia. According to Ivanonv, this is not a governmental penalty, but rather a civilian role. Despite the State Duma's requests for such actions, the Foreign Ministry has previously said that it does not favor economic sanctions. Russian merchants hold a substantial portion of Estonia's transport company, and they would bear the brunt of broad public condemnation. Concurrently, the whole political elite delivered a speech identical to Ivanov’s. Indeed, Foreign Minister Sergey Viktorovich Lavrov described the relocation of the memorial as a blasphemy that would have major ramifications for Russia's ties with Estonia[73]. In a speech at the military parade commemorating the 62nd anniversary of the Great War's victory, President Vladimir Putin even claimed that those who try to ruin memorials to war heroes are disrespecting their own people by fostering division and a new mistrust between governments and peoples, referring of course, to the events that occurred at the same time in Estonia[74]. Finally, the Russian President's First Deputy Press Secretary backed up the rhetoric, saying that there is no way the Russian state is involved in cyberterrorism because the IP addresses show where the attacks originated and show that they emerged from a diverse range of countries around the world. However, because IP addresses may be forged, this does not imply that foreign governments were behind the assaults[75]. Eventually, they demanded the resignation of Andrus Ansip's government and the restoration of the Bronze

[71] NATO, ‘2007 cyber-attacks on Estonia’, (2007), accessed on June 2nd, 2021

[72] The Baltic Times, ‘Here we go again’, (2007), https://www.baltictimes.com/news/articles/17635/, accessed on June 1st, 2021

[73] The Ministry of Foreign Affairs of the Russian Federation, https://www.mid.ru/en/main_en, accessed on June 2nd, 2021

[74] President of Russia, ‘Speech at the Military Parade Celebrating the 62nd Anniversary of Victory in the Great Patriotic War’, (May 2007), http://en.kremlin.ru/events/president/transcripts/24238, accessed on June 1st, 2021

[75] BBC News, ‘The cyber raiders hitting Estonia’, (May 2007), http://news.bbc.co.uk/2/hi/europe/6665195.stm, accessed on June 2nd, 2021

Soldier monument to its former location. Thus, the Russian reactions have two facets: the first is one of denial, in which the authorities refuse to recognize any responsibility, and the second is one of condemnation, in which they criticize Estonian actions and threaten economic retaliation.

Chapter 3: Outcomes of the 2007 cyber-attacks

The cyberattacks on Estonia in 2007 prompted a reorganization of Estonian society to coincide with the repercussions of new technology. Social, legal, and, most importantly, security developments have occurred. The country has also attempted to discover the individual responsible but has been unable due to the nature of cyberspace.

A) Strengthening of the Estonian E-society and the security of digital infrastructure

i. Early development of a nationwide cyber security and cyber defense system

Before 2007, Estonia had little capacities in cybersecurity, no national cyber strategy and the only courses provided were on cryptography, which accounts for only 2% of what cybersecurity entails[76]. The cyber-attacks of April 2007 modified Estonia's strategy towards cyber security, as they revealed the danger to the nation's digital society. Indeed, over the last decade, Estonia's capability to deal with cyber emergencies has risen exponentially and early development of a nationwide cyber security and cyber defense system for infrastructure and society have been developed. Creating national defenses to guard against potential threats became a central component of foreign policy, and Estonia became one of the first countries to enact a national Cyber Security Strategy in response to the July 2007 Action Plan to Fight Cyber-attacks submitted to the Government by the Ministry of Economic Affairs and Communications[77]. The plan intended to enhance emergency preparedness procedures in view of cyber-attacks by creating a cyber security strategy, taking into account the unique existence of cyberspace and linking it to existing defense strategies.

Therefore, the country's first strategy was introduced in 2008 and included the years 2009–2013; the second targeted the years 2014–2017 but was extended to 2018; and the new strategy covers the years 2019–2022. The first strategy created domestic processes and structures to guarantee an effective division of labor and inter-agency collaboration[78]. The second placed a

[76] Interview with Professor Rain Ottis

[77] RIA, 'Cabinet Approves Action Plan to Fight Cyber-attacks', (July 2017), https://www.ria.ee/en/news/cabinet-approves-action-plan-fight-cyber-attacks.html, accessed on May 25th, 2021

[78] ENISA, 'Cyber Security Strategy', (2008), accessed on May 25th, 2021

strong focus on critical infrastructure protection, cybercrime prevention, and information security competency development[79]. It also created the legal framework for assuring cybersecurity, international collaboration, and the growth of the cybersecurity sector of the economy[80]. The latter builds on the precedents and emphasizes four main goals; Estonia is a long-term electronic society built on technological resilience and emergency response, the Estonian cybersecurity industry is powerful, creative, research-oriented, and highly competitive, encompassing all of Estonia's core competencies. In the international arena, Estonia is a reliable and competent ally and a cyberliterate nation with a plentiful and forward-thinking talent supply[81]. Furthermore, it seeks to ensure the safety of information networks that underpin critical resources, to strengthen the battle against cybercrime, to improve national cyber-defense capability, to manage emerging cybersecurity risks, and to develop cross-sectoral operations[82]. These core priorities have been influential in developing strategies to identify and combat cyber-attacks, designing new tools to defend the Estonian government and community, and providing a large forum for international cooperation.

Moreover, in 2009, the government created a Cyber Security Council to ensure easier collaboration among different Estonian agencies in charge of the defense of information infrastructure and to monitor the execution of the Cyber Security Strategy's goals. One of its missions was to safeguard critical services from cyber challenges. A few of the measures that resulted from this include the military's development of protective cyberwarfare capability to assist Estonia's CERT and the Information System Authority's attempts to detect service weaknesses[83].

Estonia has also implemented the CIIP, the Critical Information Infrastructure Protection, whose goal is to keep the country's critical information and communication infrastructure[84] running smoothly. The Information System Authority (RIA) is given the role to coordinate national protection for the public and private sector information and network systems that are critical to the

[79] ENISA, '2014-2017 Cyber Security Strategy', https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf, accessed on May 26th, 2021
[80] RIA, 'Cyber Security', https://vm.ee/en/cyber-security, accessed on May 26th, 2021
[81] RIA, '2019-2022 Cyber Security Strategy', https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf, accessed on May 26th, 2021
[82] Stephen Herzog, 'Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity', (2017), https://www.researchgate.net/publication/326986589_Ten_Years_after_the_Estonian_Cyberattacks_Defense_and_Adaptation_in_the_Age_of_Digital_Insecurity, accessed on May 25th, 2021
[83] Ibid. 57
[84] **Glossary**

Estonian state's operation. The CIIP goals are to gather and manage data on critical information infrastructure (CII), compile reports on CII risks, develop safety protocols, create guidelines, provide relevant advice and make suggestions to service providers for risk analysis and more effective implementation of security measures, and raise cyber awareness[85]. With this structure in place, Estonia is now more protected and prepared for cyber-attacks than it was in 2007.

Furthermore, the Estonian government enacted a cybersecurity bill in 2018 with the goal of improving the institutions that provide critical services to society as well as protecting state and municipal networks and information systems. The bill also stipulates the responsibilities of the national regulatory authority, the RIA, in coordinating cybersecurity and arranging cross-border cooperation. Essential service operators, such as critical service providers, key infrastructure firms, the Estonian Internet Foundation, and key suppliers of digital services are required to implement risk-based organizational, physical, and information technology security measures. They must also monitor behaviors that endanger security and, where appropriate, take steps to mitigate the effect and spread of events[86]. A need to inform the RIA of severe cyber events was also imposed. This act is therefore a further step towards a more protected society.

Additionally, Locked Shields, a yearly scenario-based, real-time network defense exercise, involves training security specialists who secure national IT systems. It is the world's largest and most sophisticated international technical cyber defense exercise, organized by the CCDCOE in Tallinn since 2010[87]. Every year, groups are placed under severe pressure to keep a fictional country's networks and services operational. Managing and reporting problems, overcoming technical difficulties, and reacting to legal and strategic communications and scenario injects are all part of this. Locked Shields focuses on realistic technology, networks, and attack tactics to keep ahead of industry trends. In addition to educating IT professionals, Estonia is working to educate schools, governmental workers, and the general public about the dangers of cyberspace. As a result, the Estonian society is better informed, trained and equipped to deal with cyber threats and is more resilient to cyber-attacks.

[85] RIA, 'Critical Information Infrastructure Protection CIIP', https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html, accessed on May 26th, 2021

[86] Riigi Teataja, 'Cyber Security Act', (2018), https://www.riigiteataja.ee/en/eli/523052018003/consolide, accessed on May 26th, 2021

[87] CCDCOE, 'Locked Shields', https://www.ria.ee/sites/default/files/content-editors/RIA/cyber_security_in_estonia_2020_0.pdf, accessed on May 6th, 2021

Estonia has also encouraged international cybersecurity cooperation to provide high-level national protection against cyber threats through the exchange of knowledge and experience, the promotion of trust and respect, and the building of alliance and partnerships. To that end, Estonia has established bilateral and multilateral contacts with foreign nations, participates in agreed-upon cooperative activity in international organizations, and interacts with the business sector.

The attacks of 2007 have thus allowed Estonia to develop intrusion detection and protection systems, collaboration with both public and private organizations. They were also the reason why user awareness increased.

ii. Legal and sociocultural changes

The 2007 cyber-attacks have transformed the Estonian society in addition to improving cybersecurity and cyber defense systems. They disturbed Estonian society, but it was still able to quickly recover, improve and secure itself. However, due to a lack of sufficient legal authorities and institutions for addressing cyber events, Estonia experienced challenges in conducting investigations and prosecutions following the 2007 attacks[88].

One of the major issues was that Estonian laws barred certain monitoring and investigative techniques of alleged crimes if a sentence resulted in less than three years in jail. At the time, practically all cybercrimes were within this category[89]. Due to these constraints and attribution concerns, Dmitri Galushkevich was the sole culprit sentenced for the DDoS attacks. Galushkevich was fined 17,500 kroons ($1,650) for banning Prime Minister Ansip's political party's website[90]. As a result, it became clear that the government needed more than military fortification to protect itself against hackers. Estonia needed a legislative framework not just to discourage cyberattacks, but also to detect and prosecute offenders if deterrence failed. Among the most important developments in Estonian law was the revision of the country's penal code to penalize criminal actions involving computers that did not appear to be motivated by monetary gain[91]. A number of

[88] Ibid. 57

[89] CCDCOE, ‘Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security’, (2011), https://ccdcoe.org/library/publications/estonia-after-the-2007-cyber-attacks-legal-strategic-and-organisational-changes-in-cyber-security/, accessed on May 26th, 2021

[90] The Guardian, ‘That cyberwarfare by Russia on Estonia? It was one kid... in Estonia’, (2008), https://www.theguardian.com/technology/blog/2008/jan/25/thatcyberwarfarebyrussiaon, accessed on May 26th, 2021

[91] COE, ‘Estonian cybercrime legislation and case-law. Responses to the 2007 cyberattacks’, https://rm.coe.int/16802fa07e, accessed on May 26th, 2021

clauses in the amended criminal code deal with cyberattacks and cybercrime. The code defines new computer-related criminal offenses, establishes harsh sentencing rules for cybercrimes, including jail time, and establishes the Information System Authority with expanded monitoring and investigative capabilities. Illegal Internet activities are also included on the list of probable terrorist crimes in the penal code. Overall, the Estonian legal institutions that arose in the aftermath of the Bronze Soldier incidents inspired and molded international cyberlaw research.

As seen by the topic of legislation amendments in Estonia, the government frequently takes the lead in effective and preventative cybersecurity policy. However, official operations alone are useless since safeguarding against digital risks necessitates a broader sense of community awareness and alertness. In a digital world, there is a need for public awareness. As a result, the Ministry of Economic Affairs and Communications published its 'Digital Agenda 2020 for Estonia' in 2014. This paper acknowledges that more than 90% of Estonians have simple internet access and other ICT[92]. Overall, the plan highlights a national program to teach, retrain, and inform the population on a continuous basis through government efforts, public-private partnerships, and social verification of quality standards.

Moreover, the Estonian Information Technology Foundation for Education offers cybersecurity training program to the whole society regardless of age, whether through programming workshops for youth or seminars for the seniors. Tallinn University of Technology and Tartu University collaborated with the foundation to develop a new master's program in cybersecurity, which welcomed its first group of students in 2009[93]. These learning opportunities assist to guarantee that the country has a workforce of cybersecurity specialists who are well prepared.

As a result of the 2007 attacks, Estonian society has learnt to reinvent itself in order to withstand future attacks. The events of 2007 strengthened it and enabled it to carve out a new place on the world stage.

[92] Estonian Association of Information Technology and Telecommunications, 'Digital Agenda 2020 for Estonia', (2014), http://old.itl.ee/public/files/DigitalAgenda2020_Estonia_ENG.pdf, accessed on May 26th, 2021

[93] Ibid. 57

B) Charging and attribution of the attacks

The attribution of cyber-attacks is the operation consisting of monitoring, trying to identify, and blaming the perpetrator of a cyberattack or other hacking activities[94]. However, because cyberspace is immaterial and made up of grey zones, it appears to be exceedingly difficult to attribute an objectionable behavior in a specific way at the time. The attribution procedure is never totally trustworthy. The strategies employed by hackers to conceal themselves and leave few evidence make attribution extremely difficult. Technical assessments are no longer sufficient for attribution purposes since various actors employ the same techniques, tools, and operational methodologies in their activities. However, this attribution is required to go toward a judicial and political remedy, allowing for enhanced security in cyberspace.

In the Estonian case and according to the Asymmetric Threats Contingency Alliance (ATCA), an association of international experts based in London, it is the Russian authorities who have directly contributed to this. They would have rented millions of computers, used to defend Russian interests[95]. As per ATCA, the botnets were only hired for a brief time in order to increase the number of attacking machines to over a million. Nevertheless, there is no evidence to support such a claim. If Moscow did not actively coordinate the attack that shut down all Estonian institutions, it most certainly allowed it to happen, but it is hard to justify that these attacks came from the Russian territory, or to discuss a probable coordination of acts by a government service[96]. The argument over the role of Russian authorities continues to rage in the West, although it is widely believed that the state gave its approval to these attacks since there are various plausible explanations for Russia's strike on Estonia. It might have aimed to exert influence on Tallinn authorities following the removal of the Bonze Soldier statue, to test Russian cyberwarfare capabilities, or to see NATO's reaction when one of its allies is attacked.

[94] Linda Rosencrance, ‘Cyber attribution’, https://searchsecurity.techtarget.com/definition/cyber-attribution, accessed on May 27th, 2021

[95] Iain Thomson, ‘Russia 'hired botnets' for Estonia cyber-war’, (June 2007) https://www.itnews.com.au/news/russia-hired-botnets-for-estonia-cyber-war-82600, accessed on May 27th, 2021

[96] Sarah Vogler, ‘Russia’s Approach to Cyber Warfare’, (September 2016), https://apps.dtic.mil/sti/pdfs/AD1019062.pdf, accessed on May 27th, 2021

Although the cyberattacks were coordinated and the IP addresses of the targets and the dates of the strikes were accessible on Russian websites, there was no proof that the Russian government was in command[97]. The attacks might have been launched by activists on their own initiative. Yet, the magnitude of the operation and its flawless organization make it more plausible that Russian authorities were engaged, with at least implied approval from the President. The Estonian authorities stated that among the attackers were IP addresses from Russian central government systems[98]. Russia's participation is apparent in Estonia.

Besides, following the start of the riots and cyberattacks, the Russian Federation Council called for the severing of diplomatic relations with Estonia as well as the application of economic penalties. Police did not interfere when Russian nationalist youth groups invaded the Estonian embassy in Moscow and an unofficial embargo on the border between the two states also hampered trade[99]. Despite all these elements, there is no definitive confirmation of the Russian government's level of engagement as of today. Furthermore, the Russian government has always unequivocally declared that they have no link with these cyberattacks. Here we see a hallmark of cyberwarfare: the difficulty in identifying the attacker and, more importantly, in supplying the elements that confirm it. In other circumstances, the attacker may want us to believe it is them despite their inability to verify it.

In all cases, only one person was convicted, a 20-year-old Estonian student, Dmitri Galushkevich. He said he used his personal computer to perform a denial-of-service strike that pulled down the Web site of Estonia's prime minister's political party for many days. He had to pay a fine of 17,500 kroons that is to say €1300[100]. Galushkevich is the only individual to have been condemned since the April and May 2007 hacking that took down the websites of banks, schools, and government organizations. The Estonian case shows us how difficult the attribution is, especially when the hackers are outside the attacked state.

[97] Olivier Ricou, 'chapitre 7, la cyberguerre', http://www.ricou.eu.org/e-geopolitique/internet_chap8.pdf, accessed on May 27th, 2021

[98] The New York Times, 'Estonia says cyber-assault may involve the Kremlin', (May 2007), https://www.nytimes.com/2007/05/17/world/europe/17iht-estonia.4.5758556.html, accessed on May 28th, 2021

[99] Ibid. 71

[100] Jeremy Kirk, 'Student fined for attack against Estonian Web site', (January 2008), https://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012500064.html, accessed on May 28th, 2021

PART 2: Estonia's new role on the international scene: norm entrepreneur

We will see how Estonia has leveraged the 2007 cyberattacks to forge a new reputation on the worldwide stage as a forward-thinking state in the realm of cybersecurity, thanks to a nation branding strategy. Then, we'll have a look at Estonia as the source of various cyber standards, including the two versions of the Tallinn manual. We will also examine President Ilves' participation in the larger process of nation branding before addressing the dissemination of norms to more important entities such as the UN, NATO, and the EU.

Chapter 1: Establishing new norms

The cyber-attacks of 2007 allowed Estonia, to create its own new role on the international scene. Estonia took advantage of the media coverage generated by these unprecedented attacks against a state, to publicize its strengths in cyber security. Thanks to a successful strategy of nation branding and the help of NATO, it was able to be at the origin of the creation of new standards for the cyber space which materialized in the form of the Tallinn manuals.

A) Estonia as a norm entrepreneur

i. The Estonian nation branding

The concept of 'nation branding' refers to the establishment of an image and a reputation for a country. Geoffrey Wiseman, an American professor, describes it as '*the application of corporate marketing concepts and techniques to countries, in the interests of enhancing their reputation in international relations*[101]'. In short, nation branding is a subcategory of soft power using cultural, political and social values. Countries use it to diffuse a particular image of themselves around the world. This concept comes from the marketing world and designates the capacity of a country to

[101] Geoffrey Wiseman, 'Diplomacy in a globalizing world*:* theories and practices', (2013), page 354

‘sell’ its personal brand to the world and make it as accepted, appealing and welcoming as the other countries. This long process is only centred on crafting a good reputation[102].

Nation branding is the path Estonia took after the 2007 cyber-attacks. The country has illustrated itself in the fast and successful development of cyber defense and cybersecurity organisations, and legal frameworks, protecting both public and government systems. Therefore, Russia appears to be the driving force behind Estonia's digital nation-branding strategy[103].

The process was made possible thanks to the involvement of the Ministry of Defense, and the Ministry of Economy and Telecommunications which permitted for an efficient system to be put in place. Furthermore, under the command of the Ministry of Economy, the ‘Riigi Infosüsteemi Amet’ (RIA), the Estonian Information System Authority established in 2011, is in charge of the country's security, and is in charge of maintaining Estonia’s critical infrastructure[104]. The RIA is supported by the Computer Emergency Response Team (CERT), responsible for responding to potential attacks and scanning networks for potential vulnerabilities. In addition, the Estonian process is characterized by the establishment of a cyber self-defence group in 2007, the ‘küberkaitseliit’ whose main specificity lies in its integration into the army corps, although it is a civilian and voluntary organization[105]. Moreover, to ensure its leadership in the field of innovation and digital technology, Estonia has been working to export its e-democracy system and solutions such as X-Road[106] to Finland, Azerbaijan and the Faroe Islands[107]. This service represents a force of Estonian influence abroad. Thus, cyber and the new technologies in general are the main domains that allow Estonia to be notable at the European and international levels.

On the other hand, the country has embarked on a media strategy by talking publicly about the innovative projects being conducted in Estonia. The first example of this strategy was in 2012, when the country started making headlines around the world and fascinated TV cameras about its ‘little tigers,’ children who are learning to program. The explosion of the ‘tigers’ case’ marked the

[102] Melissa Aronczyk, ‘How to Do Things with Brands: Uses of National Identity’, (2009), page 294
[103] Léa Ronzaud, ‘E-Estonie” : le “nation-branding” numérique comme stratégie rayonnement international’ (2020), https://www.cairn.info/revue-herodote-2020-2-page-267.htm, accessed on April 12th, 2021
[104] Republic of Estonia Information System Authority, ‘State information system in Estonia’ (2007), https://www.ria.ee, accessed on March 16th, 2021
[105] Kadri Kaska, ‘The Cyber Defence Unit of the Estonian Defence League’ (2013), https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf, accessed on April 12th, 2021
[106] **Glossary**
[107] E-Estonia, ‘Interoperability Services’, https://e-estonia.com/solutions/interoperability-services/x-road/, accessed on April 13th, 2021

beginning of a media hysteria for Estonia and its innovations[108]. Thus, the media game in which Estonia has engaged, in addition to its strong presence in the field of innovation, e-services and international security, has offered it a role as a model and innovative country.

ii. Establishing norms in cybersecurity

Norms are all the rules of conduct that are imposed on a social group. In International Relations Theory, norms are seen as a '*standard for appropriate behavior for actors with a given identity*'[109] or '*collective expectations about proper behavior for a given identit*y'[110]. A norm differentiates from an idea, which is an individually held belief. A norm surpasses the personal sphere of beliefs and has the quality of an intersubjective, collectively held expectation about suitable conduct. On the international scene, these are the principles states abide by to maintain peace and security. In the cyber context, they are the codes that apply to behavior in cyberspace. Lately, there has been a demand for 'cyber norms' to protect and administer cyberspace.

Martha Finnemore and Kathryn Sikkink in *International Norm Dynamics and Political Change* start by explaining how and why some international norms are efficiently supported, spread and accepted by states in the international community. They describe the cycle in which norms entered once they are created: their life cycle, in which they distinguish three stages. Initially, a norm must emerge, and this process occurs when a norm entrepreneur appears with a belief that something must be reformed. Usually, this new norm uses existing organisations (i.e., The United Nations, NATO) and norms as a platform from which to spread, framing their issue to touch a wider audience. In this first stage called '*norm emergence'*, states endorse a norm for national political motives. If enough states adopt the new norm, a '*tipping point*' is reached, and the norm moves to the second stage. The second stage is called '*norm cascade*' because states accept a norm in response to international pressure. They adopt the norm to increase their internal needs for legitimacy, conformity and esteem, as being seen as non-conformist by the international

[108] Ibid. 35
[109] Martha Finnemore, Kathryn Sikkink, 'International Norm Dynamics and Political Change' (1998), https://www.jstor.org/stable/2601361?seq=1, accessed on April 10th, 2021
[110] Thomas Risse, 'International human rights norms and domestic change: conclusions' (1999), https://www.cambridge.org/core/books/power-of-human-rights/international-human-rights-norms-and-domestic-change-conclusions/6822537228C126F25EE1B2332BCF9FD5, accessed on April 11th, 2021

community makes them appear inferior. Finally, the third stage, '*norm internationalization*', occurs when compliance to the norms becomes so usual that states stop to even observe the presence of a norm. It is therefore a long and arduous process for a norm to be adopted by the whole international community.

There are five main reasons a norm is more likely than the others to reach the tipping point. The first is legitimacy, states tend to adopt new norms when their legitimacy vacillates. They embrace new international norms when they seek to enhance their reputation or esteem. The prominence of a norm is also important. If a norm is adopted by all prominent states, then it is more likely to be adopted by others as well. Norms that value universalism and individualism are also those most likely to be accepted by the international community. Furthermore, if a new norm looks like or is derived from an older accepted norm, then it is also more likely to be endorsed on the international scene. Finally, the more unstable the international system is, the more likely is a search for and acceptance of new ideas and norms.

Because of its small size as a state and its absence of noteworthy military power, Estonia has had to find its own way to exert its influence on other states. Thanks to its successful nation branding strategy, it has established itself as a norm entrepreneur in cybersecurity. After the 2007 cyber-attacks Estonia has started to diligently encourage and reinforce cyber norms and ask for acceptance from the international community. Estonia is therefore the main player during the first stage in the life cycle of norm, norm emergence. However, as mentioned before, Estonia is not a leading state in the international community and has rather limited resources to maintain its security. That is why Estonia has had to align with NATO to influence the advertising of cyber norms in the international community. It uses the organizations to vocalize its beliefs on how states should behave in cyberspace. NATO has given Estonia a platform to support the types of norms Estonia is interested in enacting[111].

The three central categories Estonia has been supporting abroad are internet regulation, e-governance, and cybersecurity. However, Estonia's objectives of forming cybersecurity norms are broader than just promoting the issue of cybersecurity. It is paramount for Estonia to see that a

[111] Matthew Crandall, Collin Allan, 'Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms', (2015), https://www.tandfonline.com/doi/abs/10.1080/13523260.2015.1061765?journalCode=fcsp20, accessed on March 14th, 2021

certain type of norm is being established. The cybersecurity norms that Estonia is promoting can be divided into two groups both linked to sovereignty issues. First is the openness of the internet stressed by Estonia's membership in the Freedom Online Coalition, a group of 32 governments working together to advance internet freedom[112]. The second part of the cybersecurity norms is about the responsibility of state in cyberattacks. Estonia wants to expend the responsibility of states in cybersecurity. Estonia is thus establishing itself as the architect and sponsor of international legal norms in the fields of cyber operation and cybersecurity. To this end, it uses all existing procedures, including its participation in NATO. Estonia has been active in organizing international cyber exercises and hosting the NATO CCD-COE which resulted in the publication of the Tallinn Manuals, that we will further discuss.

In 2014, the Estonian Ministry of Economic Affairs and Communication reformed the country's cyber strategy for the years 2014-2017. It acknowledges the progress Estonia has achieved and highlights several targets regarding the establishment of cybersecurity norms. This new strategy asks Estonia to be a cyber-norm entrepreneur as well as it is a part of the norm-development course[113]. Estonia was the second country, after the Russian Federation to produce a cybersecurity strategy. 16 European countries have since implemented cybersecurity strategies which shows how Estonia's advocacy in the EU and NATO played a key part[114]. Estonia was successful in bringing attention to the question of cybersecurity and trying to persuade others to adopt the new cyber norms as well.

Since, the advertising of cybersecurity norms has become a duty of the state, many Estonian state representatives are supporting cybersecurity norms on a regular basis in front of large audience. For instance, Urmas Reinsalu, a former minister of defence, has put forward the topic on several occasions, especially with NATO. Urmas Paet, the past minister of foreign affairs has also referred to the issue[115]. Among all the state officials who have backed for cybersecurity, the most powerful person in Estonia has been President Ilves, whose major role will be discussed

[112] Freedom Online Coalition, 'About Us', https://freedomonlinecoalition.com/about-us/about/, accessed on April 10th, 2021

[113] Ministry of Economic Affairs and Communication, '2014-2017: Cyber Security Strategy', (2014), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf, accessed on April 1st, 2021

[114] Ibid. 43

[115] Ibid. 43

in a further chapter. We will here, underline how Estonia has utilized its participation in NATO as an organizational platform to bring attention to cybersecurity. For example, in 2010, in NATO's Strategic Concept document, cybersecurity was a central subject[116]. At the 2014 Wales summit, NATO recognised the Enhanced Cyber Defence Policy, which acknowledges cyber-defence to be part of NATO's collective defence mission[117]. This means that a NATO country has the right to invoke article five[118] in the event of a cyberattack. This constant elaboration of cybersecurity norms is in part due to Estonia's cybersecurity endorsing efforts. According to Ilves' security consultant, five countries are viewed as agenda-setters when it comes to cybersecurity and Estonia is one of them while the rest are bigger and more prominent states, it is therefore quite remarkable for Estonia to be part of this group[119].

The biggest symbol of Estonia's achievement in NATO is the creation of the NATO Cooperative Cyber Defence Center of Excellence (CCD-COE) in Tallinn. It was recognized by NATO in 2008, just a year after the cyber-attacks against Estonia. Its mission is to '*enhance the capability, cooperation, and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultations*.'[120] The centre has issued over 85 studies and articles with many Estonian scholars. One of the most noteworthy success in establishing norms has been the publication of the Tallinn Manuals that we will discuss in the next part. Along with the enabling of the production of the Tallinn Manuals, the CCD-COE has given the Estonian institutions and researchers opportunities to contribute to the norm promotion process. Thus, NATO membership has given Estonia the opportunity to bring cybersecurity to the international agenda. Estonia has also been highly

[116] NATO, 'Strategic Concept 2010', (2010), https://www.nato.int/cps/en/natolive/topics_82705.htm, accessed on April 11th, 2021

[117] NATO, 'Wales Summit Declaration' (2014), https://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease, accessed on April 11th, 2021

[118] NATO, 'The North Atlantic Treaty', (1949),*'The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.' https://www.nato.int/cps/en/natohq/official_texts_17120.htm*

[119] Josh Gold, 'Estonia as an international cybersecurity leader', (August 2019), https://e-estonia.com/estonia-as-an-international-cybersecurity-leader/, accessed on April 2nd, 2021

[120] CCDCOE, 'About Us', https://ccdcoe.org/about-us/, accessed on March 24th, 2021

effective in getting the support of NATO's former secretary general and has been successful in realizing practical advancements.

iii. What differentiates the Estonian and Georgian cases?

The cyber-attacks that occurred in 2008 in Georgia and in 2007 in Estonia have many similarities, yet Estonia has established itself in the international community as a cyber-norms entrepreneur while Georgia does not play a major role in promoting cyber-norms, why is it?

The cyber-attacks in Georgia were different from the attacks in Estonia because they were the precursors of an armed conflict. They took place months before the outbreak of war. In July 2008, DDoS attacks against Georgian websites were recorded. On August 8th, new attacks were recorded but on a much larger scale, they coincide with the entry of Russian forces in South Ossetia[121]. There were two phases to the attack, the first was focused on Georgian news and government websites. Unlike the Estonian case, Georgian IT systems were less robust and therefore suffered more damage. The second phase targeted financial institutions, businesses and educational institutions[122]. Until August 10th, the majority of the Georgian governmental websites were defective, and the government was incapable to correspond with the world using the internet. As for Estonia, the attacks came from the Russian territory, but experts did not find a clear direction between the Russian authorities and the attacks. It is interesting to note that the Georgian case differs from the Estonian one in the sense that the cyber-attacks were coordinated with conventional attacks on the ground. However, there remains similarities between both attacks. Both countries had a tensed relationship with Russia, it is clearly that these attacks were politically motivated. The attacks were also of the same type: DDoS attacks, but in the Georgian case they were more sophisticated. Another resemblance is the object of the attack. The websites of government were disrupted as well as the domains of banks and online newspapers. Both countries were also dependent on the internet and were more susceptible to cyber-attacks. Finally, because of the architecture of cyberspace, it is impossible in both cases to determine who is at the origin of the attacks. After these attacks, Estonia has been able to impose itself on the international scene,

[121] John Markoff, 'Before the Gunfire, Cyberattacks', (August 12th, 2008), https://www.nytimes.com/2008/08/13/technology/13cyber.html, accessed on April 15th, 2021

[122] Ibid. 53

while Georgia has remained in the shadows and has not tried to take on a more prominent role. This can be explained by the fact that Estonia has more international contacts. Estonia has been a member of the European Union and NATO since 2004. Georgia, on the other hand, is not a member of the European Union and has applied to join NATO, but no decision has been made yet regarding its membership. Estonia, through these different international organizations, has therefore more opportunity to find a platform to disseminate its ideas on how cyberspace should be ruled. This example shows us that the initial will of a state is necessary but not sufficient. Estonia has built a reputation of a very advanced nation in the cyber domains, but this process alone would not have been enough, it needed the platform of NATO provided.

B) The Tallinn Manuals

i. The Tallinn Manual on the International Law Applicable to Cyber Warfare

The *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn Manual) was created at the initiative of the NATO Cooperative Cyber Defence Centre of Excellence (CCD-COE) and intends to be a manual for managing cyberwar. The manual is one of the earliest, most enduring, and most recognized research initiatives launched by the CCD-COE.[123]. It is well worth mentioning that the centre is only accredited by NATO, meaning it runs exercise, education, and research in support of NATO missions. Thus, the Manual does not have an official nature, nor does it represent the opinions of NATO[124].

The CCD-COE gathered an international group of legal academics and specialists under the direction of Michael N. Schmitt, an American international law scholar specialized in international humanitarian law, use of force issues and the international law applicable to cyberspace[125]. Together they worked on the draft of the Tallinn Manual which tackles a number of significant problems in the interpretation of international law. The group completed three years of work on

[123] Cooperative Cyber Defence Centre of Excellence, 'Tallinn Manual Process' (2017), https://ccdcoe.org/research/tallinn-manual/, accessed on April 6th, 2021

[124] Michael Schmitt, 'The Tallinn Manual 2.0 on the International Law of Cyber Operations: What it is and isn't' (9 February 2017), https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/, accessed on April 5th, 2021

[125] University of Reading, 'Michael Schmitt', https://www.reading.ac.uk/law/Staff/m-schmitt.aspx, accessed on April 5th, 2021

the application of existing international legal norms to cyber warfare. The manual was published in March 2013 by the University of Cambridge and encompasses themes such as the rightful reasons to go to war *(jus ad bellum*), the rules to be followed during the war (*jus in bello*), and international law governing the issue of resorting to force with regards to the national policies of states. It contains the analyses of the independent expert group. It offers a valuable basis for measuring the extent to which international law applies to cyber operations. The manual focuses on the most significant and critical cyber operations from a national security perspective, those that violate the ban of the use of force in international relations, allowing states to exercise the right to self-defence[126] and brings clarity to the complex legal issues surrounding these operations.

It is based on three major objectives. The first is to interpret existing international norms by applying them to cyberattacks, as there was no common interpretation of treaties to cyber operations prior to this manual. The second is to reconnect the cyber-technical and legal worlds in their analysis and understanding of each other. The last is to gauge the ability of states to seek consensus on ethical and legal boundaries in cyberspace, especially on what is meant by armed aggression or use of force[127].

When strictly applying international law to relations between states in the context of cyber operations, it is considered that a state is sovereign and responsible for the control of cyber infrastructures on its territory. The two main difficulties deal with, on the one hand, the assessment of the responsibility of a State on whose territory a cyber operation is being prepared and, on the other hand, the qualification of the cyber operation as a violation of the principle of sovereignty[128]. In regard to the use of force in cyberspace, the Tallinn Manual analysis gives a qualitative and quantitative factor:

> ‘*A cyber operation constitutes a use of force when its scale (degree/threshold of intensity) and effects are comparable to a traditional (non-cyber) operation that would have reached the level of use of force.*’[129]

[126] Ibid. 34
[127] Oriane Barat-Ginies, ‘Existe-t-il un droit international du cyberespace ?’ (2014), https://www.cairn.info/revue-herodote-2014-1-page-201.htm, accessed on April 7th, 2021
[128] Ibid. 37
[129] Michael Schmitt, ‘Tallinn Manual on the International Law Applicable to Cyber Warfare’ (2013), Part I, chapter 2, Rule 11’Definition of use of force’, https://www-cambridge-org.myaccess.library.utoronto.ca/core/books/tallinn-

Moreover, according to the Tallinn Manual, the interpretation and qualification of armed aggression can be transposed to cyber conflicts. This choice was proposed by the experts in order to maintain a high threshold of qualification of aggression and to avoid that any hostile act launched in the cyber domain leads to an armed (non-proportional) response by the victim state. Thus, the proposed formula is to accept the right to self-defence when the state has been targeted by a cyber operation that has reached the level of intensity of an armed aggression (beyond the qualitative and quantitative criteria for the use of force). Furthermore, the cyber operation constitutes armed aggression when the use of force reaches a high threshold in terms of degree, level of intensity, and effects generated. When the use of force results in loss of life, injury to persons, or damage to property, the threshold for classification as "armed aggression" will be met. However, the experts in the manual did not quantify this threshold and no international cyber incident to date has met the threshold of qualifying as an armed attack[130]. Even the cyber-attack in Estonia in 2007.

In the cyber context, the experts agreed that a state should not wait passively for the attack to take action when it is imminent. Some experts consider that the criterion of temporality should be analyzed: distinguishing between the preparation of the action and what constitutes the first phase of the attack. Others, like Michael Schmitt, have proposed the theory of the *last window of opportunity*[131]. According to this analysis, self-defence will be used before the attack is launched, because it is the absence of intervention that will cause the incapacity of the victim state to act against the attack. Three criteria are to be assessed: the actors conducting the attack, their intent and capabilities, and the irreversible nature of the attack.

This Manual is therefore very insightful as it shows that international law is not silent on new technological developments and helps states in assessing the legality or unlawfulness of cyber operations. However, not all states agree on the importance of the manual. Reflecting the divergent representations of cyberspace between Russia and the West, an official of the Russian Ministry of Defense, Konstantin Peschanenko, said:

manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE, accessed on April 5th, 2021

[130] Michael Schmitt, 'Tallinn Manual on the International Law Applicable to Cyber Warfare' (2013), Part II, https://www-cambridge-org.myaccess.library.utoronto.ca/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE, accessed on April 5th, 2021

[131] Ibid. 34

> '*The issue of cybersecurity is the most topical at the moment. It is especially important to prevent the militarization of the cyberspace, while the Tallinn manual is a step in this direction. Its approach to the issue is far from perfect. And the assessments made in seem to be one-sided*'[132].

According to the Russians, it is the Atlanticists from NATO who are instrumentalizing cyberspace. So, it seems that the manual is more of a western representation than a global representation of cyberspace law. It is thus a first step towards the regulation and clarification of the cyberspace, but it is necessary to go further and include more researchers and viewpoints from different geopolitical actors.

ii. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Tallinn 2.0) was released in February 2017 and published by Cambridge University Press as an extension of the scope of the Tallinn Manual and measures the applicability of international law to cyberspace activities. The original Manual concentrated on what qualifies as an armed attack, what falls under the threshold for the use of force in armed conflict and thus allows states to respond in self-defence, and what happens during armed conflict. Fortunately, such cyber-attacks have not yet occurred in real life. Instead, the majority of malicious cyber operations have taken place far below the threshold of armed conflicts between states and have not risen to the level that would trigger such a conflict[133]. Therefore, Tallinn 2.0 deals with more common cyber incidents that countries face on a day-to-day basis. It expands upon the original piece by adding critical and legal analysis of international law to cyber activities and operations that are shorter and less violent than actual warfare and occur during peace time. It also includes more information on the role of cyber weapons and equipment in the cyber fight. In short, the first one was looking at war while this one

[132] Jakob Magnusson, 'The question of preventing cybercrime against governmental institutions', https://www.unodc.org/unodc/index.html, accessed on April 7th, 2021
[133] Eric Talbot Jensen, 'The Tallinn Manual 2.0: Highlights and Insights' (13 March 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2932110, accessed on April 6th, 2021

focuses on peace time and operations that fall ‘below the threshold’ of the use of force and armed conflict[134].

Rather than being doctrine, the manual is an analysis of how international law applies to cyber operations in the view of 19 members of the ‘International Group of Experts’(IGE). This group, in response to criticism, was more diversified than the first one, including scholars from China, Thailand, Belarus and Japan specialized in domains such as international telecommunication law and space law[135].

Tallinn 2.0 is separated into four segments. The first segment is about general international law and cyberspace. The second touches on specialized regimes of international law and cyberspace. The third covers international peace and security and cyber activities which mostly come from the initial Tallinn Manual. Finally, the last segment is composed of Tallin 1.0. It is then composed of 2 types of text. The first type is ‘black letter rules’ which required unanimity and are meant to reflect *lex lata*, the law as it is, not *lex ferenda*, the law as it should be. On the other hand, with extensive commentary providing definitions, explanations and opinions among the IGE as to the application of the rule and its interpretation. For instance, for the *Rule number 70 – Definition of threat of force*, the Experts agreed on the following Black letter rule:

> *‘A cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force.’*[136]

However, it is latter mentioned that the IGE was divided as to whether a State noticeably lacking any abilities to make good on its threat can violate this Rule. There was therefore no consensus regarding a State that possesses the capability to carry out the threat but clearly has no intention of doing so. This passage shows how the experts dealt with the absence of consensus.

[134] Ibid. 34

[135] Ibid 43.

[136] Michael Schmitt, ‘Tallinn Manual on the International Law Applicable to Cyber Operations’ (2017), Part III, chapter 14, Rule 70 ’Definition of threat of force’, https://www-cambridge-org.myaccess.library.utoronto.ca/core/services/aop-cambridge-core/content/view/F2871424CF6758F2C9275568B777DF51/9781316822524c14_p328-356_CBO.pdf/use_of_force.pdf, accessed on April 5th, 2021

The manual also discusses, the legality of activities such as a nation hacking into a nuclear power plant of another country and holding it hostage, threatening to blow up the plant and kill large numbers of people unless the nation withdraws from an unrelated conflict, believing that would be a violation of international law[137]. The experts also interpret the traditional protections of the Geneva Convention for prisoners of war in the cyber age and suggest that it is expressly forbidden to publish humiliating or degrading information collected from prisoners or images taken of them in detention on the Internet[138]. The concept of 'cultural property' and the digitization of physical artifacts are also receiving attention. In the past, the destruction of a nation's or people's cultural heritage could deprive them of an essential link to their past. In today's digital world, this heritage is increasingly digitized, meaning that even if the original photograph, statue, building or other work is destroyed by occupying military forces, the object will survive as a digital memory[139].

Finally, despite the rapidly evolving world of deep learning and autonomous warfare, the textbook focuses primarily on a cyberenvironment populated by human actors and spends little time on legal issues related to fully autonomous cyberweapons capable of fully independent decision making and how they might fit into the concept of international law. This might be analysed in a further version.

iii. The Manuals as tools to propel Estonia to the international scene

The publication of both Tallinn 1.0 and 2.0 was remarkable for Estonia in the sense that for the first time since the country's independence from the Soviet Union in 1991, the name of its capital city had been put on the world's mental map of international law through a long and accomplished project. The releases of the Tallinn Manuals in 2013 and 2017 is one piece of a large body of evidence that Estonia, as an independent state, has made a name for itself in the international community and is acknowledged by this community. At the same time, this handbook is a sign that Estonia has reached a certain level of maturity as a state. In fact, mature states do not focus

[137] Kalev Leetaru, 'What Tallinn Manual 2.0 Teaches Us About The New Cyber Order' (9 February 2017), https://www.forbes.com/sites/kalevleetaru/2017/02/09/what-tallinn-manual-2-0-teaches-us-about-the-new-cyber-order/, accessed on April 7th, 2021
[138] Ibid. 46 Part III, Chapter 15, Rule 79 'Peace operations personnel, installations, materiel, units and vehicles'
[139] Ibid. 47

selfishly on their own affairs, but rather try to contribute to solving the problems of the international community as a whole. One expression of this maturity is the willingness to contribute to the research about the challenges such as cyberwarfare and cyberconflict, that international law faces. Tallinn 1.0 and 2.0 have therefore given greater visibility to Estonia. Global citizens no longer have to look up online what Tallinn means, as the Estonian president ironically remarked in an interview for an American channel[140].

The manuals are also an analytical response from Estonia to the 2007 cyber-attacks and other cyber operations that have occurred around the world subsequently and may have been sanctioned at the governmental level. By reading between the lines of the Tallinn Manual, one would find that the state or its agents who ordered the cyberattacks against Estonia in 2007 may have committed an illegal act under international law, regardless of the fact that it was not an armed attack under the UN Charter[141]. So, the manuals are a way to gain visibility on the international scene but also to assert Estonia's answer against the 2007's cyber-attackers.

In 2021 building on the success of the first two versions, the CCD-CoE launched the process to update the Tallinn Manual once again. It will include revision of all chapters of Tallinn 2.0 to address the evolving nature of cyber operations and state responses. Tallinn will remain active in the cyber international community.

[140] TheCyberDiplomat, 'Tallinn Manual – A Brief Review of the International Law Applicable to Cyber Operations' (6 December 2019), https://medium.com/@cyberdiplomacy/tallinn-manual-a-brief-review-of-the-international-law-applicable-to-cyber-operations-5643c886d9e2, accessed on April 5th, 2021

[141] Lauri Mälksoo, 'The Tallinn Manual as an international event' (8 August 2013), https://icds.ee/en/the-tallinn-manual-as-an-international-event/, accessed on April 5th, 2021

Chapter 2: Toomas Hendrick Ilves, Estonia’s norm-building agent

During the 2007 cyber-attacks, the Estonian President, Toomas Hendrick Ilves, played an important role in establishing Estonia as a standard setter in the cyber domain. With his curiosity and interest in new technologies, he has established himself as an important figure on the international scene and was able to influence international organisations and other states.

A) President Ilves and the concept of a norm-building agent

i. Ilves as President and his interest in Information and Communications Technology

This part was written using the biography section of the former Estonian president's website[142]. In 2006, Toomas Hendrik Ilves was elected fourth President of the Republic of Estonia. In 2011, he was re-elected for a second mandate. Duringhis presidency, he was assigned to several high-level posts in the European Union in the field of Information and Communications Technology (ICT). For instance, from 2011 to 2012, he was the Chairman of the EU Task Force on eHealth, which sought to make suggestions on what should be done to ensure that Europe earns the full benefits of eHealth by 2020[143]. He served as Chairman of the European Cloud Partnership Steering Board, which aims to provide guidance on cloud computing production in the European Union[144], from 2012 to 2014, at the request of the European Commission. President Ilves also served as co-chair of the advisory panel for the World Bank's World Development Report 2016 *‘Digital Dividends’* from 2014 to 2015, and as chair of the World Economic Forum's Global Agenda Council on Cyber Security from June 2014 to May 2016.

His interest in computers and ICT began at a young age, and thanks to that early curiosity he has been fostering Estonia's IT growth since the country regained its independence in 1991. President Ilves has spoken and written widely on integration, transatlantic ties, e-government,

[142] Toomas Hendrik Ilves, ‘Biography’, https://www.presidentilves.ee/bio, accessed on May 18th, 2021
[143] European Commission, ‘EU Task Force on eHealth: Redesigning health in Europe for 2020’, https://ec.europa.eu/digital-single-market/en/news/eu-task-force-ehealth-redesigning-health-europe-2020, accessed on May 18th, 2021
[144] European Commission, ‘European Cloud Partnership’, https://ec.europa.eu/digital-single-market/en/european-cloud-partnership, accessed on May 18th, 2021

cyber security, and other related subjects. At the time he was the Estonian Ambassador to the United States, in 1995, he launched a revolutionary effort to promote e-skills in Estonia. He is thus widely seen as the father of the famous *'Tiger Leap Program'*, which served as a facilitator for a number of large-scale digital projects aimed at establishing the internet as the mainstream medium in all aspects of society. Young people were the first to profit from the *'Tiger Leap Program'*, which linked schools to the internet, provided them with the requisite hardware and software, and provided teachers with adequate preparation.

He won the Digital Freedom Award in 2016 in recognition of his efforts to promote digital democracy and raise awareness of the possibilities and problems that the digital age would bring[145]. President Ilves has written several essays and papers on security policies and cyber security in both Estonian and English such as *The Consequences of Cyber-Attacks* for the Journal of International Affairs of Columbia in 2017[146] in which he says that Estonia showed that even small developing or emerging countries can capitalize on the Internet's benefits by pursuing a smart and systematic digital growth strategy. Estonians have built and used technology solutions, gaining useful insight in how to secure these facilities and, more broadly, how to protect the way we live. He concluded by saying that cybersecurity is a benefit and not a hindrance.

The involvement of President Ilves has enabled him to establish himself as an important and indispensable norm building agent in Estonia.

ii. Ilves as a norm building agent

President Ilves throughout his mandates and even after has helped Estonia to create the Estonian reputation as a global cyber-norm entrepreneur and has sought to gain a spot on the international stage for his and Estonia's ideas about cybersecurity norms. As such, he can be considered as an individual norm entrepreneur or a norm building agent. The role of the entrepreneur is not only to help create new standards, but to preserve them over the long term. President Ilves' participation was extremely crucial following the attacks because it helped to

[145] Estonian World, 'Ex-president Ilves receives the Digital Freedom Award', (November 2016), https://estonianworld.com/technology/ex-president-ilves-receives-digital-freedom-award/, accessed on May 18th, 2021

[146] Columbia SPIA, 'The consequences of cyber attacks', (June 2017), https://jia.sipa.columbia.edu/consequences-cyber-attacks, accessed on May 18th, 2021

promote Estonia's case in the international arena and, because Estonia is a tiny country, it served to further protect the country by making it visible[147].

Cass Sunstein, an American legal scholar, used the term *'norm entrepreneur'* in his 1996 essay *Social Norms and Social Roles*[148]. He observes that current social conditions are frequently more precarious than is commonly thought, since they depend on social standards with which many people do not closely identify. Typically, social expectations are rooted in a network of social roles, social situations, and legal codes. And, as a consequence of collective action issues, risk aversion, or the weakness of the human imagination, these norms can continue even when many people oppose or hate them. The scholar defines a group of people he labels norm entrepreneurs as those who are involved in reforming social norms. If their attempts are active, it may set off a chain reaction, '*norm cascade'*, that eventually leads to significant shifts in an entire society's social norms. Norm entrepreneurs can take advantage of widespread frustration with current norms to drive society toward a new norm in a variety of ways, including signaling their own contribution to reforming norms, forming coalitions, questioning norms that tend to be the least costly, and making conformity with new norms appear more advantageous.

Therefore, a norm entrepreneur must also solve the problems of collective action, that is to say a situation in which all the individuals would have interest in cooperating but do not do it because of contradictory interests between the individuals which discourage the common action[149]. Here the common action would be the emergence and the perpetuation of the standards. As the Estonian president, he can enforce the standards and propagate them at the international level through meetings between states or within international organizations and thus solve the problem of collective action. This has been done mainly in official announcements and public addresses at national and international universities, in talks with heads of state and international conferences.

[147] Interview with Visiting Fellow at Canadian International Council Josh Gold, June 7th, 2021

[148] Cass R. Sunstein, 'Social Norms and Social Roles', (1996), https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1455&context=law_and_economics, accessed on May 24th, 2021

[149] Katharina Holzinger, 'The problems of collective action: A new approach', (2003), https://www.econstor.eu/bitstream/10419/85085/1/2003-02_online.pdf, accessed on May 24th, 2021

B) Analysis of President Ilves's statements

In the case of Estonia, President Ilves has been a central player in the dissemination of new cyberspace and cybersecurity standards created within his country. In this part will have a closer look at his addresses and speeches, using the 'Speeches and Writing' section of his website[150]. He has commented on a variety of Internet-related matters, but I will draw my attention to his remarks on cybersecurity, as well as the role of NATO and the United States in cybersecurity.

After a closer look at his statements, it appears that Ilves has advocated for cybersecurity across five major channels: university lectures, international event presentations, addresses at or to international bodies, meetings with other state officials, and important leadership roles in working groups. These initiatives discussed both the need to take cybersecurity more seriously and the need to establish cyber norms. Besides, these different platforms provided Ilves with access to elites who are crucial to the norm promotion process[151]. Ilves shows his capacity to act as a norm-building agent by drawing attention to the situation by discussing these two subjects.

As we will see in the next chapter about the dissemination of cyber standards, Estonia has had to rely on international organizations, including NATO, in order to establish itself as an entrepreneur of standards in the cyber domain. Therefore, we will see how the statements of President Ilves have allowed Estonia to shine at the international level, but how they have been addressed directly or indirectly to the major international organizations so that they act in favour of Estonian ideas[152]. For instance, Ilves addressed the North Atlantic Council in Tallinn in May 2014, emphasizing the importance of NATO advancing cyber training and exercises[153]. He also stressed the importance of increasing cyber interoperability. The United States has been a particularly valuable focus for Ilves' cyber-advocacy since it represents a great power with strong soft and hard powers, which Estonia lacks. As such, he went several times to the United States. He

[150] Toomas Hendrik Ilves, 'Speeches and Writing', https://www.presidentilves.ee/speeches, accessed on May 24th, 2021

[151] Peter Schraeder, 'Elites as Facilitators or Impediments to Political Development?', (1994), https://www.jstor.org/stable/4192413?seq=1, accessed on May 24th, 2021

[152] Matthew Crandall, Collin Allan, 'Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms', (2015), https://www.tandfonline.com/doi/abs/10.1080/13523260.2015.1061765?journalCode=fcsp20, accessed on March 14th, 2021

[153] Republic of Estonia, 'All NATO ambassadors to visit Estonia for the first time', (May 2014), https://vm.ee/en/news/all-nato-ambassadors-visit-estonia-first-time, accessed on May 24th, 2021

alerted the students at the National Defense University in Washington DC about the risks of cyberattacks and hackers' power to momentarily weaken state networks[154]. In a speech at Harvard University in 2012, he emphasized the importance of NATO taking cyber-defense more seriously, as well as the need for the EU and NATO to work together on this subject[155]. In a visit to President Obama in 2009, Ilves raised the question of cybersecurity, praising the US for its assistance after the 2007 attacks and working hard to keep cybersecurity on the US agenda[156]. Ilves' attention to the United States has reaped many benefits: on December 3, 2013, the United States and Estonia concluded a Cyber Partnership Statement[157]. This relationship commits Estonia and the United States to expanding their collaboration on three cyber topics: cybersecurity, e-governance, and internet freedom and governance. Although the United States works with several countries on these issues, this was the first substantive agreement signed by the United States, demonstrating that the United States regards Estonia as a significant partner. This close relationship has not prevented him from continuing his efforts, in 2017 he gave a speech before the Senate Judiciary Subcommittee on Crime and Terrorism, in which he expressed his opinion on the new weapons that ICTs represent and how Russia is using them to undermine democracies all around the world[158].

Ilves has also called for cybersecurity standards at international conferences. He participated in cyberspace conference in London in 2011[159], where many country leaders were present including Russia, China and the United States. He also attended a cyber conference in

[154] NDU, 'Estonian President Addresses National Defense University Students', (August 2013), https://www.ndu.edu/News/Press-Releases/Article/572587/estonian-president-addresses-national-defense-university-students/, accessed on May 24th, 2021

[155] Toomas Hendrik Ilves, 'President Ilves at Harvard University: all members of NATO must share a common understanding of cyber security', (April 2012), https://vp2006-2016.president.ee/en/media/press-releases/7314-president-ilves-at-harvard-university-all-members-of-nato-must-share-a-common-understanding-of-cyber-security/layout-visit.html, accessed on May 24th, 2021

[156] Estonian World Review, 'President Ilves met with President Obama', (June 2009), https://www.eesti.ca/president-ilves-met-with-president-obama/article24169, accessed on May 24th, 2021

[157] US Department of State, 'The United States and Estonia: Partners in Cyber Security and Internet Freedom', (December 2013), https://2009-2017.state.gov/r/pa/prs/ps/2013/218234.htm, accessed on May 24th, 2021

[158] Toomas Hendrik Ilves, 'Prepared Testimony and Statement for the Record of Toomas Hendrik Ilves', https://www.judiciary.senate.gov/imo/media/doc/03-15-17%20Ilves%20Testimony.pdf, accessed on May 24th, 2021

[159] Toomas Hendrik Ilves, 'President Ilves to attend an international conference in London devoted to e-solutions and cybersecurity', (2011), https://vp2006-2016.president.ee/en/media/press-releases/6677-president-ilves-to-attend-an-international-conference-in-london-devoted-to-e-solutions-and-cybersecurity/layout-visit.html, accessed on May 24th, 2021

Budapest in 2012[160] and another one in Helsinki in 2013[161], and he regularly speaks at the NATO CCDCOE's annual International Conferences on Cyber Conflict. He said at the 2014 Munich Cyber Security Conference that cybersecurity goes way further than the conventional military security framework, that it means securing whole nations[162]. The Freedom Online Coalition Conference was the most significant event he attended. In 2014, Estonia organized the meeting, and Ilves emphasized the importance of upholding Internet independence as well as reaching a strategic agreement on cyber issues, which is required for developing global strategies[163].

President Ilves has since spoken out in favor of cybersecurity standards at a number of international bodies. At the United Nations, he stressed the value of net neutrality and reiterated that internet security should not be used to limit internet freedom. Ilves has been thinking about the EU as well. In a meeting with Cecilia Malstrom, the European Commissioner for Home Affairs at the time, in 2012, Ilves emphasized the importance of the EU developing a shared cyber strategic plan[164]. In addition to his speeches at international organisations, he has an influence through his leadership positions on committees and working groups. Ilves presided over a Cyber Security Council meeting at the invitation of the World Economic Forum. Therefore, his capacity to influence and foster cybersecurity standards has grown thanks to these leadership roles.

Ilves played a major role in the establishment of Estonia as a norm entrepreneur. His work exemplifies how an individual can draw attention to a specific topic. He publicized to the topic by stressing the importance of increasing cyber-defence capability and collaboration, as well as the need to develop codes of ethics to regulate cyber behavior. He was therefore crucial for Estonia.

[160] Toomas Hendrik Ilves, ‘President Ilves spoke at cyber conference in Budapest’, (2012), https://vp2006-2016.president.ee/en/media/press-releases/8042-president-ilves-spoke-at-cyber-conference-in-budapest/index.html, accessed on May 24th, 2021

[161] Toomas Hendrik Ilves, ‘President Ilves to give an opening address at the high-level CyberStrat conference in Helsinki’, (2013), https://vp2006-2016.president.ee/en/media/press-releases/8475-president-ilves-to-give-an-opening-address-at-the-high-level-cyberstrat-conference-in-helsinki/index.html, accessed on May 24th, 2021

[162] Toomas Hendrik Ilves, ‘Rebooting Trust? Freedom vs Security in Cyberspace’, (2014), https://vp2006-2016.president.ee/en/official-duties/speeches/9796-qrebooting-trust-freedom-vs-security-in-cyberspaceq/, accessed on May 24th, 2021

[163] Toomas Hendrik Ilves, ‘Remarks by the President of Estonia, Toomas Hendrik Ilves at the Freedom Online Coalition Conference in Swissotel’, (April 2014), https://vp2006-2016.president.ee/en/official-duties/speeches/10101-remarks-by-the-president-of-estonia-toomas-hendrik-ilves-at-the-freedom-online-coalition-conference-in-swissotel-april-28-2014/index.html, accessed on May 24th, 2021

[164] Ibid. 102

Chapter 3: 'Norm cascade': dissemination of standards to international organizations

After the success of the first stage of norms establishment, norms emergence', Estonia has embarked on the second stage, 'norm cascade'. To do this, it relied on the largest international organizations of which it is a member. We will look at how the cyber-attacks of 2007 changed the security strategies of NATO, the EU and the United Nations and we will evaluate the direct impact of Estonia in these changes.

A) Estonia in the North Atlantic Treaty Organization

i. The Alliance before the 2007 cyber-attacks

Long before the 2007 cyber-attacks against Estonia, NATO had measures in place to protect its communications and information systems. The initiative started after the events that happened in the late 1990s, during the NATO Operation Allied Force in Kosovo. The Alliance was attacked by pro-Serbian hacktivists who wanted to destroy NATO war capabilities, only the Alliance's website and some email addresses were blocked[165]. As a result of these events, Alliance leaders agreed at the 2002 Prague Summit to craft a cyber defense program, that led to the creation of the NATO Computer Incident Response Capability (NCIRC), which aims to defend Alliance networks, detect potential attacks in cyberspace and provide information and assistance to users[166]. The attacks at that time were still considered as not very harmful or damaging, the responses created was viewed as sufficient. The following years have seen the development and sophistication of communication and information systems, creating new vulnerabilities and insecurities for member states.

The 2007 cyber-attacks against Estonia were a real wake-up call for the Alliance as they demonstrated that cyber-attacks could greatly damage a nation dependent on the internet. At the time, as a member of the Alliance, Estonia had called on it to defend itself from persistent attacks against digital infrastructures. These attacks represented the first major case of cyber-attacks

[165] Benjamin S. Lambeth, 'Operation Allied Force: Lessons for the Future', (2001), https://www.rand.org/pubs/research_briefs/RB75.html, accessed on April 19th, 2021

[166] NATO, 'NATO Cyber Defence', (July 2016), https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-en.pdf, accessed on April 19th, 2021

against a NATO member state, much larger than those that occurred in 1999 during the Kosovo operation. They were also a blow to the Alliance because they showed that NATO lacked a cyber doctrine, a strategy for cyber space, and that its Cyber Defence Program was no longer sufficient to meet contemporary needs[167]. The attacks against Estonia forced the Alliance to rethink its strategy to better manage the growing threat from cyber space. Estonia has played a major role in the establishment of NATO's clear objectives and official position in the event of cyber-attacks against one of the member states because it showed that cyber-attacks were a tangible threat to NATO member states, especially as countries are increasingly dependent on IT networks. That is why in 2010, the NATO Strategic Concept which is the NATO's statement on its values and objectives for the next decade, after recognizing that cyber-attacks are becoming more frequent and organized, emphasizes that the alliance will:

> *'develop further its ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations'*[168].

However, before defining a formal policy, NATO needed to address some of the issues that emerged from the 2007 attacks.

ii. The emergence of new challenges in cyber space

The 2007 attacks raised new questions that needed to be addressed before developing a formal strategy. These questions can be grouped into three sub-categories: legal, operational and strategic[169]. From a legal point of view, the central issue was whether cyber-attacks could trigger the collective defense mechanisms of Articles 4 and 5 of the 1949 Charter, which give the

[167] NATO, 'Five years after Estonia's cyber-attacks: lessons learned for NATO?', (May 2012), https://www.files.ethz.ch/isn/143191/rp_76.pdf, accessed on April 19th, 2021

[168] NATO, 'Strategic Concept for the Defence and Security of the members of the North Atlantic Treaty Organization', (November 2010), point 19, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf, accessed on April 19th, 2021

[169] Ibid. 76

presumably attacked state the prerogative to determine whether it is under attack or threat. The problem with these articles is that there is no clearly defined threshold above which a state can consider itself under attack in the cyberspace, so it would have to be decided individually by studying each case. Invoking these articles would then depend on political motivations. Another important legal point is the responsibility of a state, when cyber-attacks have been launched from its territory. International law recognizes the responsibility of a state when it does not respect its international obligations, but it is responsible only if it has explicitly agreed not to respect its obligations. In the case of Estonia, can we hold Russia responsible for the attacks knowing that the majority of them came from its territory? This question remains unanswered. Finally, a last legal issue is the application of humanitarian law to cyber-attacks.

The second subcategory, operational, showed that the Alliance's cyber defense capabilities needed to be upgraded. The NCIRC was no longer sufficient to manage all attacks against NATO networks or to help allies protect their critical digital infrastructure. Finally, at the strategic level, it was necessary to create an entirely new strategy because those that applied to other strategic fields could not simply be transposed. For example, deterrence[170] is essential in NATO's strategy. It is built through two different processes: denial, which is based on the technological superiority of the Alliance in the face of the adversary, which allows it to have effective and strong solutions and punishment that involves retaliation greater than the initial attack. However, deterrence by punishment is difficult to apply in cyber space because its particular structure and involvement of different actors makes it difficult to attribute attacks to a particular state. Furthermore, it is difficult to determine which infrastructures to target and what threshold determines the use of deterrence. Once these challenges were tackled, the Alliance was able to embark on the development of a strategy to address threats in cyber space.

iii. Improvements to take an active role in cyber threat management

Even though the attacks were a hard blow to the Alliance, they were actually a blessing in disguise, they allowed NATO to improve and strengthen its strategy and policy in cyber space to face new threats. For example, at the operational level, in 2008 at the Bucharest summit cyber defence was defined as NATO’s core task of collective defence and a new cyber policy was presented to the

[170] Ibid. 75

allies which set up the Cyber Defence Management Authority (CDMA)[171] to coordinate and initiate cyber defence actions where necessary. It was later replaced by the Cyber Defence Management Board (CDMB), which represents the central command for political and technical actions and knowledge and information sharing, as well as the entity that directs the various cyber defense structures within NATO. The Alliance has thereafter recognized that its main mission in cyber defense is to protect its own networks and build resilience across the Alliance[172]. In July 2016, an important threshold was crossed as allies recognized cyberspace as an operational field on the same level as land, sea and air[173]: cyberspace is therefore defended as much as they are. In 2018, at the Brussels summit, a cyber operations center integrated into the NATO command structure was created and member states agreed that the alliance could draw on the national capabilities of each state to launch missions[174]. Finally, in 2019 in an effort to improve NATO's capabilities to respond to major cyber-attacks, the allies adopted a manual in which the Alliance's tools are presented. In addition to the operational level, NATO also worked on the doctrinal level by strengthening its partnerships with states outside the alliance and within the private sector to find complementary solutions and avoid unnecessary duplication. The creation of the CCDCOE in Tallinn and the publications of the Tallinn Manuals were also big steps towards the establishment of a clear doctrine.

Therefore, after the 2007 attacks, NATO strengthened its capabilities and developed a cyber-strategy. The Alliance is now better equipped to deal with cyber operations. Estonia has thus had a direct role in creating the awareness that led to this process. Moreover, the fact that the Alliance is better prepared to counter cyber threats is an advantage for Estonia's security as well as for its strategic position within the Alliance[175]. Estonia carved out a niche for itself that it uses in its favor. Estonia is like an '*incubator*'[176] that can continue to inform NATO on security issues related to

[171] Europarl, 'Defending against cyber-attacks', https://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede251010audnatocyberattacks_/sede251010audnatocyberattacks_en.pdf, accessed on April 19th, 2021

[172] Ibid. 75

[173] NATO, 'NATO's role in cyberspace', (February 2019), https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html, accessed on April 19th, 2021

[174] NATO, 'Brussel Summit Declaration', (July 2018), https://www.nato.int/cps/en/natohq/official_texts_156624.htm, accessed on April 19th, 2021

[175] RKK ICDS, 'How Estonia uses Cybersecurity to Strengthen its Position in NATO, (May 2019), https://icds.ee/en/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/, accessed on April 19th, 2021

[176] Ibid. 84

technological advances and the effects of those advances on democracy and society. Estonia's ideas and experiences provide valuable models and test cases for the Alliance and ensure that Estonia remains valuable to the Alliance.

B) Estonia in the European Union

i. Estonia as a trigger for the European cybersecurity strategy

The European interest in cyberspace is not new and this is because most of the states of the Union are members of NATO. The trigger element was the same as that of NATO, meaning the cyber-attacks carried out by Serbian hackers against the website of the Supreme Allied Command Europe of NATO. These events prompted the European Union (EU) to address cyberspace in the same way as NATO. The European Commission launched a series of directives in the early 2000s to protect the fundamental rights and freedoms of European citizens in the context of online economic and commercial activities[177]. This economic dimension has long prevailed in European standards relating to the cyber domain. The 2003 European Security Strategy, for example, made no mention of cyber threats[178]. The cyber-attacks against Estonia and Georgia in 2007-2008 prompted a new stage of reflection and, in February 2013, the EU adopted a cybersecurity strategy[179], the subtitle of which advocates an open, safe and secure cyberspace. This strategy aims to make the Union resilient to cyber-attacks and makes cyber defense one of the five priorities to be developed at the European level.

In recent years, the EU has developed strategic documents aimed at establishing itself as an actor in the regulation of cyberspace, including in the military and diplomatic fields. In particular, a framework of action for a joint EU diplomatic response to cyber-malicious activities also known as the ‘cyber-diplomatic toolbox’[180], was adopted by the European Council in June

[177] Delphine Deschaux-Dutard, ‘L’Union européenne : une cyber puissance en devenir ? Réflexions sur la cyber défense européenne’, (2010), https://www-cairn-info.scd-rproxy.u-strasbg.fr/revue-internationale-et-strategique-2020-1-page-18.htm#no8, accessed on April 20th, 2021

[178] Consilium, ‘A Secure Europe in a better world: European Security Strategy’, (December 2003), https://data.consilium.europa.eu/doc/document/ST-15895-2003-INIT/en/pdf, accessed on April 20th, 2021

[179] Ibid. 86

[180] Consilium, Cyber-attacks : EU ready to respond with a range of measures, including sanctions’, (June 2017), https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/, accessed on April 20th, 2021

2017, with a view to coordinating responses to cyber-attacks and enabling the adoption of sanctions against the attackers. This capability was deepened in May 2019, demonstrating a real European will to exist as a diplomatic actor in cyberspace.

Cyber defense, on the other hand, is the military component of the EU's external action in the cyber domain. The European cybersecurity strategy includes cyber defense for the first time in the EU's defense activities, which are brought together under the Common Security and Defense Policy. This strategy also invokes the possibility of using the solidarity clause contained in the Treaty on the Functioning of the EU[181] in the event of a cyber-attack: *'A particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause'*[182]. Finally, the EU Cyber Security Strategy identifies four priorities for European cyber defense: developing capabilities and a framework for a cyber defense policy in coordination with member states, promoting civil-military dialogue on cyber issues, and dialogue with international partners such as NATO[183]. However, the strategy remains rather vague and has required the adoption of complementary standards to advance cyber defense on a European scale.

From a strategic point of view, it seems more and more obvious that the EU is beginning to position itself as a security actor in cyberspace, even if the economic dimensions and those related to political freedoms still largely mark European thinking on the subject. Since a strategy is only effective if it is given the means, the EU is also developing some related cyber defense tools.

ii. The new European tools against cyber threats

The EU has developed several types of tools in parallel with its cyber defense strategy. First of all, there are legal tools provided by the European treaties, such as the mutual defense clause[184] or the solidarity clause mentioned earlier. Although these two clauses do not expressly refer to cyber defense, they could be invoked in the case of a cyber-attack that crosses the threshold of armed

[181] TFEU, Article 222: *'The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilize all the instruments at its disposal, including the military resources made available by the Member States'*

[182] 3.2 EU support in case of a major cyber incident or attack, page 19

[183] Ibid. 86

[184] Article 42§7 of the Treaty on European Union*: 'If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defense policy of certain Member States.'*

cyber conflict, meaning that has lethal consequences and causes damage of the same nature as an attack by conventional weapons. However, the use of the mutual defense clause would raise the same difficult question that arises for NATO: attributing the cyber-attack to a state or non-state actor. Such attribution would first require a consensus within the European Council, which would produce difficulties. It is therefore more the solidarity clause that seems to provide an avenue for cyber defense in the short term, because a large-scale cyber-attack, which cannot be considered an armed attack, can be similar to a natural disaster, allowing Member States to ask for help from the Brussels institutions and their European partners. In operational terms, this would mean logistical and material assistance, provided by the European institutions and the other member states, to the affected State to restore the affected computer networks or to attribute the source of the attack[185].

A second type of tool allows for the progressive development of the European cyber defense capabilities. This is the Permanent Structured Cooperation (PESCO), an institutional tool for cooperation between a group of voluntary states launched in December 2017, and which now has more than 13 projects dealing with cyberspace issues[186]. This cooperation will, for example, allow the creation of Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity[187], giving the opportunity to develop exercises and training and to better coordinate responses to cyber-attacks that have military implications. However, once again, unanimity is required.

In addition to these legal and institutional tools, there is a third type of tool: cyber-diplomacy. The EU not only conducts several cyber-dialogues with strategic partners such as the United States, China, India or NATO, but can also, since May 2019, impose sanctions. Cyber-attacks that may be subject to European sanctions are those originating outside the territory of the EU, using non-EU infrastructure, conducted by entities established outside the EU and conducted with the assistance of entities operating outside the EU. However, they come up against the same problem as the previous tools: the need for a consensus between member states to determine who is responsible for the cyber-attack. The European Union was able to take a new turn after the cyber-attacks of 2007, but it seems that the tools it developed are not effective enough because of the European Union's own decision-making mechanisms. Therefore, some authors argue that the EU

[185] Ibid. 86
[186] PESCO, 'PESCO About us', https://pesco.europa.eu, accessed on April 20th, 2021
[187] EU Cyber Direct, 'Cyber-related PESCO projects', (November 2019), https://eucyberdirect.eu/content_knowledge_hu/cyber-related-pesco-projects/, accessed on April 20th, 2021

should focus on the development of a *'cyber soft power'*[188], which would make the Union a normative power in cyber space. The EU Cyber Net initiative, which aims to bring experts together on cybersecurity issues to develop expertise, is a step in this direction.

iii. How can Estonia assist the European Union?

Estonia, thanks to its experience in 2007 and the expertise it has gained from it, is an asset for the European Union. Estonia must identify the existing strengths of the Union and develop them. There are three points on which Estonia could assist the European Union. First, it should help the Union to strengthen cooperation between the public and private sectors as it has already done nationally with the Cyber Defence League (CDL). The CDL's main objective is to defend the information infrastructure and to develop national defense objectives. The interesting point is that the CDL is composed of specialists, experts but also volunteers with IT skills, so the research benefit the public sector as well as the private sector[189]. This working structure should be recalled at the European level.

Second, the European Union should be inspired by the Estonian model because it considers the resilience of computer networks a strategic priority. Unlike cybersecurity, which focuses on preventing and combating cyber threats, resilience is the ability to manage the disruption of services without too much disruption to society. Security is paramount, but in the event of an attack, resilience is even more important.

Finally, the last point on which the EU should continue to focus is that of offensive capabilities. The EU may engage in research, but it should primarily guide and direct it. In this regard, it must once again look to Estonia, which has established itself on the international stage as a cyber norm entrepreneur. So, the best thing Estonia can do is to convince the EU to join it in its standards-building efforts[190]. The Estonian events have thus favored the development of a European cyber security strategy, but Estonia still has a role to play in perfecting it.

[188] Ibid. 86

[189] CCDCOE, 'The Cyber Defence Unit of the Estonian Defence League', (2013), https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf, accessed on April 20th, 2021

[190] Emmet Tuohy, 'Towards an EU Cybersecurity Strategy: the Role of Estonia' (December 2012), http://pdc.ceu.hu/archive/00006852/01/ICDS_Toward-EU-Cybersecurity-Strategy-The-Role-of-Estonia.pdf, accessed on April 20th, 2021

C) Estonia in the United Nations

i. Estonia in the United Nations Security Council

On September 17, 1991, Estonia joined the United Nations (UN) and since May 2004, it has been a member of the Eastern European Group, one of the five UN regional groups. In May 2020, Estonia retained for the first time the presidency of the United Nations Security Council (UNSC) and raised many issues during various thematic sessions in line with its priorities as an elected member, including European security, cybersecurity, civilian population safety, and the Security Council's working methods during the Covid19 crisis. It had four main goals: holding the coronavirus epidemic in the spotlight, as the outbreak also presents a danger to global security, increasing transparency and working practices, exposing breaches of international law, and, most notably, raising the question of emerging security threats[191].

The question of cybersecurity was discussed at the UN Security Council table for the first time on March 5th at Estonia's initiative, in collaboration with the United Kingdom and the United States[192] and Estonia continued to raise concern of new challenges as president of the Council because it was time to discuss general rules for a secure and safe cyberspace, particularly now that cyber-attacks, and cybercrime had escalated as a result of the Covid19 pandemic. Estonia has therefore used its role as Council President to circulate its ideas and standards on cybersecurity. Estonia primarily believes that the Security Council must address threats to international peace and security that are now beginning to appear on the Security Council's agenda such as cyber threats. The fundamental question to consider is the Security Council's position in maintaining responsible state behavior in cyberspace. Estonia considers that defending the legitimacy of universal cyber standards and international law in cyberspace is important. Prime Minister Jüri Ratas said on May 22nd during the meeting organized by Estonia on cyber ability, cyber norms and international law:

[191] Republic of Estonia Ministry of Foreign Affairs, 'Estonia's presidency in UN Security Council' https://vm.ee/en/activities-objectives/estonia-united-nations/estonias-presidency-un-security-council, accessed on April 21st, 2021

[192] Just Security, 'Estonia speaks out on key rules for cyberspace', (June 2019), https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/, accessed on April 21st, 2021

'As a pioneering country with extensive experience in the cyber domain, Estonia wishes to ensure that the Security Council makes serious efforts to prepare for emerging threats. Now is the right time to discuss how to prevent conflicts in cyberspace and how states can protect their digital infrastructure more efficiently. The coronavirus crisis is further accelerating the digital transformation of states; however, this is why we must pay particular attention to the information systems of hospitals and other medical institutions. Online cybercrime is also still here. With our friends and allies, we must continually look for ways to keep up with various threats when ensuring our safety.'[193]

Furthermore, as we have previously seen, Estonia has considerable expertise in influencing cybersecurity strategies in international organizations such as the EU and NATO so, it could contribute to the United Nations' standard development as well.

Even though no resolution was passed during Estonia's term in the Council, Estonia was able to raise awareness at the United Nations and this was a very promising first step towards assertive actions from the UN. Furthermore, when Estonia, along with the United Kingdom and the United States, attributed a cyberattack on Georgia to Russia in March 2020[194], it helped set a precedent for taking attribution of a cyberattack to the Security Council. This serves as a powerful example of how countries should keep each other accountable for breaches of international norms, and it serves as a reminder to states that their acts have consequences. State-sponsored cyberattacks are among the most dangerous threats to peace and stability, and governments are often the targets. As a result, introducing the cyber issue to the Security Council recognizes the importance of states upholding their commitments to one another. The presidency was a good way to get the word out about cybersecurity outside the EU and NATO and to reach a wider audience of countries. It also benefited Estonia, which was again able to appear as a world leader in cybersecurity.

[193] Permanent Mission of Estonia to the UN, 'The Estonian Presidency of the UN Security Council holds a landmark discussion on cybersecurity', (May 2020), https://un.mfa.ee/the-estonian-presidency-of-the-un-security-council-holds-a-landmark-discussion-on-cybersecurity/, accessed on April 21st, 2021

[194] Ibid. 101

ii. *Estonia in the United Nations mandated working groups for international cyber stability*

The United Nations Group of Governmental Experts is a UN-mandated working group in the domain of information security which works on advancing responsible state behaviour in cyberspace in the context of international security. Since 2004, six working groups have been established, including the last GGE 2019-2021 which will submit its final report to the General Assembly in 2021. Unlike the Open-Ended Working Group (OEWG), it is only composed of 25 members and not of all the states interested in the cyber issue[195]. The OEWG is a new mechanism that arose from a Russian resolution in November 2018 to create a *'more democratic, inclusive, and transparent'*[196] body to research responsible state behavior and cooperative initiatives in cyberspace alongside the GGE. Russia pressed for this, recognizing that a bigger coalition makes it more difficult to reach an agreement, as well as to have more countries that will share its interests in cyberspace.

The GGE addresses norms, rules and principles that apply to cyberspace, confidence building measures that are not binding but prevent hostilities and how international law applies to cyberspace. The OEWG addresses existing and potential cyber threats, creates relevant international concepts for securing global IT systems and establishes regular institutional open-ended dialogue within the UN[197]. Both groups are among the most influential venues for debating global standards for responsible state behavior and recognizing that international law applies in cyberspace. Estonia participates in both of these working groups for international cyber stability.

One of the GGE's greatest successes is the application of international law to cyber space in June 2013: *'international law, and in particular the Charter of the United Nations, is applicable, and is essential in maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment'*[198]. In the report submitted in 2015, Estonia played a greater role since it focuses on norms, rules, and principles for the responsible behaviour of states. The report

[195] DigWatch, 'UN GGE and OEWG', https://dig.watch/processes/un-gge, accessed on April 21st, 2021

[196] Josh Gold, 'The First Ever Global Meeting on Cyber Norms Holds Promise, but Broader Challenges Remain', (September 2019), https://www.cfr.org/blog/first-global-meeting-cyber-norms, accessed on April 21st, 2021

[197] Ibid. 104

[198] UN, 'International Law in the Consensus Reports of the United Nations GGE' https://www.un.org/disarmament/wp-content/uploads/2020/01/background-paper-on-international-law-in-the-gges.pdf, accessed on April 21st, 2021

presents 11 new standards and values guidelines[199] among which there are limiting norms such as states should not engage in or actively promote Information and Communication Technology (ICT) action that wreaks havoc on sensitive infrastructure and positive principles that state good practice such as states should work together to improve ICT peace and protection and to discourage malicious activities. The 2015 report also adds principles to be respected in cyberspace such as sovereignty, equality between states, peaceful resolution of conflicts, non-intervention in the internal affairs of other states and respect for human rights and fundamental freedoms[200]. These two groups are very innovative, but many questions remain unanswered such as how do the established principles of international humanitarian law: humanity, necessity, proportionality, and distinction apply to cyberspace? And how does international law apply to cyber-attacks in peacetime? Estonia has once again established itself as a key player in these working groups, thus strengthening its role as a cyber norm entrepreneur on the international scene.

Estonia, thanks to its successful nation building strategy, has succeeded in establishing itself as a norm entrepreneur in the cyber domain. This new role has allowed it to be heard in all the major international organizations of which it is a member. Nevertheless, if its action within the United Nations is direct and explicit, its action within the EU and NATO was much less so. Indeed, it is at the origin of the stronger strategies in both organizations, not because it initiated them, but because the organizations were frightened by the 2007 cyber-attacks. It was only afterwards that Estonia developed its expertise and was able to establish itself as an expert, something she was able to do from the beginning in the UN.

[199] CCDCOE, '2015 UNGGE Report: Major players recommending norms of behavior, highlighting aspects of international law', https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/, accessed on April 21st, 2021 and **appendix 2**

[200] Ibid.108

PART 3: To what extend can Estonia establish itself as a world leader in cybersecurity: the limits to the Estonian influence

It will be demonstrated that despite its expanding international influence, Estonia encounters several limits. We will show that it has external limits because of its hostile neighbor, Russia, but also within the Western camp, where consensus on cyber standards is impossible to achieve since perspectives and interests conflict in such a strategic field. Second, we will see that some limits are directly related to Estonia and its lack of cybersecurity professionals as well as existing vulnerabilities.

Chapter 1: External limits

Since 2007 Estonia has managed to create a place for itself within the European and international community as an expert on the cyber issue, but it is still hampered by external limitations. Indeed, the place of Russia in the cyber space as the main opponent of its standards is difficult to mitigate because of their fundamental differences. In addition, the disagreements within the Western countries, the structure of cyberspace and the competition of the United States are obstacles to its influence.

A) The shadow of a hostile neighbor: Russia

i) A conflict in the terms used that depicts different realities

Estonia may be on Russia's doorstep, but the two countries have diametrically opposed views on cybersecurity and cyberspace. In the Western hemisphere to which Estonia belongs, when we think about cyberspace, we usually picture an imaginary digital space, in contrast to the physical world and its geography, in which boundaries are only artificially replicated and sovereign states face new challenges in managing or even governing it. Russia is the polar opposite of this Western image: its decision-makers' political perceptions of it, as well as the reality of its network's organisation, appear to demonstrate that the nation retains a view of the Internet and digital networks in which hegemony and culture are primary, and competition with the Western world is key[201].

This competition between the West and Russia manifests itself first and foremost in a semantic argument. The concept *'cyberspace'* and the way of thinking it underpins, according to Russian strategic thought, were mostly forged by American private and public institutions at the end of the 1990s, according to a paradigm of world representation largely influenced by the aspirations of globalization in the time between the collapse of the Soviet Union in 1991 and September 11, 2001[202]. As a result, in Moscow, we tend to refer to *'informational space'* rather than *'cyberspace'*. This terminological shift is far from rhetorical, since it suggests fundamental different perceptions of the Internet and the modern digital world. Indeed, the concept of informational space encompasses a far broader reality than cyberspace: it includes all platforms and ways of disseminating information, not just the Internet (television, radio, newspapers...)[203]. In reality, current Russian geopolitical analysis ignores the concept of cyberspace that will be a unique and incomparable object with its own set of governance laws. On the other hand, it views digital networks, such as the Internet, as newspapers, over which the government has regulatory authority[204]. As a result, we can deduce that the Russian conception is primarily shaped by the priority of sovereignty, which the idea of cyberspace appears to obliterate.

Furthermore, Russia sees cyberwarfare differently than its Western peers, from how it is defined to how it is used for strategic purposes. When referring to Western or other foreign writings on the topic, Russians often use the words *'cyber'* or *'cyberwarfare'*. However, they like to use the term *'informatization'*, as do the Chinese, to conceptualize cyber operations as part of a larger picture of *'information warfare'*[205]. Russian military scholars use the word information warfare to

[201] Kévin Limonier, 'La Russie dans le cyberespace: représentations et enjeux' (2014), https://www.cairn.info/revue-herodote-2014-1-page-140.htm, accessed on April 26th, 2021

[202] Ibid. 110

[203] Michael Connell, 'Russia's Approach to Cyber Warfare' (September 2016), https://apps.dtic.mil/dtic/tr/fulltext/u2/1019062.pdf, accessed on April 26th, 2021

[204] Ibid. 113

[205] Tim Maurer, 'Russia's cyber strategy', (December 2018), https://www.ispionline.it/en/pubblicazione/russias-cyber-strategy-21835, accessed on April 27th, 2021

describe a comprehensive definition that encompasses computer network operations, cyber warfare, psychological operations, and information operations[206].

In other words, cyber is viewed as a tool for allowing the state to control the information landscape and is seen as a separate warfare realm. This difference in terms has far-reaching implications. Indeed, one of the features of contemporary military conflicts, according to the Russian Federation's Military Doctrine of 2010, is the prior application of informational warfare interventions to accomplish political goals without the use of military force[207]. As a result, informational warfare tools should be used prior to the start of offensive campaigns in order to accomplish the state's goals without resorting to military action. Informational warfare and, by default, cyberwarfare, became legal state tools in both peace and war times. In this situation, information may be used to obstruct policy, mobilize anti-government demonstrations, deceive critics, sway popular sentiment, and weaken an opponent's resolve to fight. Subsequently, the cyber-offensive is reduced to a supporting role, assisting the state in gaining control of information at all levels of the war. The informational space has no spatial or temporal limits. This contrasts sharply with the Western, and thus Estonian, view of cyberspace as a distinct realm from informational warfare.

Thus, a major limitation to Estonian influence in cyberspace is its hostile neighbor, Russia. If the two countries do not agree on the terms to be used and the definitions to be given to them, how can they agree on much more specific subjects such as the application of international law to cyberspace? In order to have a real influence, Estonia must overcome the East/West distinction and have its concepts accepted by Russia. Another way would be to redevelop new concepts with Russia and not leave it out of the drafting of important texts. However, this option would force Estonia to start from scratch in the process of adopting standards on the international scene.

[206] Keir Giles, ‘Russia’s new tools for confronting the West: continuity and innovation in Moscow’s exercises of power’, (March 2016), https://www.chathamhouse.org/2016/03/russias-new-tools-confronting-west-continuity-and-innovation-moscows-exercise-power, accessed on April 26th, 2021

[207] The Military Doctrine of the Russian Federation, point 13, (d), (February 2010), https://carnegieendowment.org/files/2010russia_military_doctrine.pdf, accessed on April 27th, 2021

ii) From different concepts and representations to different systems: the Runet

Runet is the Russian-speaking segment of the Internet. In concrete terms, this refers to all websites, servers, and e-mail addresses that distribute information in Russian[208]. The Runet refers to a part of the Internet where web activities are distinct. In addition to being focused on the practice of a shared language: Russian, it also corresponds to a segment of the Internet where web practices are different. While Estonian, German, or even French users continue to use commonly used resources like Facebook or Google, Russian-speaking users prefer technologies built for and by Russians. Runet is thus differentiated not only by the language, but also by the services favored by its users, making it a market that Western corporations find difficult to access[209]. The countries of the former Soviet Union, except the Baltic States, are the countries where social networking sites like *Vkontakte* and *Odnoklassniki*, as well as the search engine *Yandex*, are widely used. Runet is also notable for the fact that the vast majority of its content is hosted on servers in Russia[210].

The Runet, thanks to its autonomy, has been the receptacle of an identity challenge in recent years. As a result, publications, blogs, and comments are thriving on the Russian-speaking Web, establishing Runet as a real *'patriotic Internet'*[211]. The Runet's autonomous nature acts as a cyberspace continuation of the effort to preserve this culture of destiny, which is heavily influenced by the Cold War's aftermath and conflict with the United States. The 2007 cyber-attacks against Estonia were precisely related to these identity and memory challenges.

The promotion of the Runet as a political space is focused on a conflict with the West and the ideals that it represents. The idea of Runet confirms the Russian quest for dissociation, supported by the independence of the Russian segment of cyberspace. It is therefore very complicated for Estonia to influence the former Soviet republics in cyberspace since Russia uses the information space to create a zone of cultural, linguistic, and political influence. The division is much deeper than a disagreement on terms.

[208] Emeline Strentz, 'La Russie dans le cyberespace : Runet est-il le nouveau rideau de fer numérique ?', (November 2019), https://portail-ie.fr/analysis/2207/la-russie-dans-le-cyberespace-runet-est-il-le-nouveau-rideau-de-fer-numerique, accessed on April 27th, 2021

[209] Ibid. 117

[210] Ibid. 110

[211] Ibid. 110

iii) The Russian offensive attitude

In addition to the semantic and systemic conflicts, Russia has adopted an offensive attitude towards the West in general and Estonia in particular. This attitude distances it from the standards advocated by Estonia and prevents the latter from fully asserting itself on the international scene. Advanced persistent threat (APT) groups, or cyber-hacking groups, have been an essential part of Russia's cyber toolset[212]. However, despite the fact that the activities of these groups are aligned with the ideas of the Kremlin, it is difficult to prove any link between these groups and the Russian government. Especially since the Russian authorities deny any responsibility for the cyber-attacks. It seems that Russia is delegating cyber operations to actors outside the government.

There are two main reasons why Russia uses intermediaries[213]. First and foremost, it is cost-effective. Intermediates don't need anything in the way of logistical support: Russia only needs to give a list of targets and attack vectors to hackers and they manage themselves without requiring any input from Russian authorities. Hackers are also easily mobilized and dismantled if they are no longer needed. Moreover, hacktivists, nationalist hackers, of whom there are many in Russia, often work for free if the issue suits their ideology. Second, hackers are suitable for working in the grey field of information warfare since they provide the Kremlin with an extra level of anonymity and exacerbate the attribution issues that come with cyberspace. Even the most detailed inquiries seldom yield obvious attributions that can be attributed to government servers or IP addresses. This is perfect for Moscow because its rivals believe the Russian government to be involved, but they lack definitive evidence to hold the Kremlin responsible.

This Russian organization, which allows it to act concealed in cyber space, is at the origin of the Russian offensive attitude. Even today, Russia keeps attacking states without being held responsible. For example, in April 2020, a Russian hacking group used forged diplomatic cables and planted articles on social media to undermine the governments of Estonia and the Republic of Georgia. The same month, Poland believed the Russian government was behind a series of cyber-attacks on Poland's War Studies University, which are part of a misinformation operation aimed

[212] Robert Lemos, ‘Russian Nation-State Hacking Unit’s Tools Get More Fancy’, (May 2019), https://www.darkreading.com/application-security/russian-nation-state-hacking-units-tools-get-more-fancy/d/d-id/1334792, accessed on April 27th, 2021

[213] Daniil Turovsky, ‘Moscow’s cyber-defence How the Russian government plans to protect the country from the coming cyberwar’, (July 2017), https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense, accessed on April 26th, 2021

at sabotaging US-Polish ties. German officials discovered in May 2020 that a Russian hacker group linked to the FSB, the federal security service, had infiltrated the networks of German energy, water, and power companies by breaching the firms' suppliers. In July 2020, Canada, the United Kingdom, and the United States revealed that Russian intelligence-linked hackers had tried to steal information relating to the creation of the Covid-19 vaccine. The French national cybersecurity agency revealed in February 2021 that a Russian hacker group was behind a four-year operation targeting French IT providers[214]. These examples are only a small part of all the cyber-attacks that have been publicly attributed to Russia, but they allow us to clearly see Russia's offensive attitude.

Russia is therefore a significant obstacle to Estonian influence in the cyber space because it defends a totally different model of cybersecurity, using different terms. Not only are their visions contradictory, but Russia continues to attack states in cyberspace and thus violates the international rules that are supposed to apply to cyberspace. It seems that this situation is hopeless in view of the antagonisms between the countries. To be successful internationally, and not just in the West, Estonia will need to integrate the Russian perspective into its thinking about setting cyber standards.

B) Disagreement within the Western hemisphere

i. Disagreement on how to rule cyberspace and multitudes of standards

Not only does Estonia have to deal with an antagonistic Russian model, but it also has to cope with the different visions within the Western countries themselves. Moreover, each of them tries to assert themselves in the cyber space and sometimes against the others. A state must target another state for security purposes and to prepare to counter an attack: this is the cybersecurity dilemma. Cyberspace is not a territory in the traditional sense of the word, but it is used as a place where people interconnect. The states, no matter how much they belong to the West, therefore, want to conquer, govern, and reclaim this territory where state boundaries, authority, and rules can be respected. According to Stéphane Dossé states must now:

[214] CSIS, 'Significant Cyber Incidents', https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents, accessed on April 27th, 2021

"'plant the flag' in the spaces they inhabit in order to exercise all of their sovereign roles, colonize virgin spaces, and be prepared to meet adversaries in this space"[215]

In other terms, cyberspace has become a military priority, and cybernetic weapons are now part of the states' arsenal. In the interest of defending their political authority and sovereignty, states must return in force to cyberspace and this, sometimes to the detriment of the established norms and rules.

The challenge of preventing cyberattacks can have an effect on their ability to maintain national security and safety. There are specific worries regarding safeguarding critical facilities, which, if destroyed or sabotaged, could put civilians at risk. Cyberspace is so strategic that it is difficult for countries to agree, even in groups that aim to produce non-binding documents. Despite two decades of political activity at the United Nations, intersubjective consensus on principles concerning repressive cyber control remains embryonic[216]. Norms that have been agreed upon and expressly specified are seen as optional, broadly described, and poorly internalized. Application contestation has been the prevailing dynamic in the cyber norms phase after the 2013 agreement that international law extends to cyberspace in general. The 2016/2017 UNGGE's mandate included a discussion of how international law applies. That was also one of the reasons for the UNGGE's demise in 2017, as members couldn't agree about whether or not to make an explicit reference in the UNGGE report stating that international humanitarian law extends to cyberspace[217]. Moreover, it was not until March 2021 that all countries of the United Nations reached a consensus on a report of guidelines for promoting cyberspace peace and stability. The study is neither legally binding nor transformative in substance, but it is the first time that a forum opened to all countries has resulted in international cybersecurity agreement although no nation was fully satisfied with the report's contents[218]. These two examples show us that states initially fail to agree on the standards to be put in place and that once they are established, they fail to agree on how to apply them. Thus, the strategic nature of cyberspace and the growing cyber-threats lead

[215] Stéphane Dossé, 'Le cyberespace - nouveau domaine de la pensée stratégique', (2013)

[216] Bart Hogeveen, 'Six years in the making: UN reaches global cyberspace consensus', (March 2021), https://www.aspistrategist.org.au/six-years-in-the-making-un-reaches-global-cyberspace-consensus/, accessed on April 30th, 2021

[217] Ibid. 125

[218] Josh Gold, 'Unexpectedly, all UN Countries agreed on a cybersecurity report? So What?', (March 2021), https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what, accessed on April 29th, 2021

to a dead end. Either the states do not agree, and nothing changes, or they agree on non-binding documents, which are intended to be strong messages, but which ultimately change nothing. It is therefore difficult for Estonia to enforce the standards it creates.

In addition to the difficulty of reaching an agreement to rule cyberspace, there is a multitude of standards developed by actors each more different than the others[219]. First, we have the states who attempts to establish cyber norms for other states, this is the case of Estonia. This process is referred to as multilateral standard diplomacy. The most visible efforts are made under the supports of the United Nations. Other bodies, such as the Shanghai Cooperation Organisation, the G7, and the G20, have also attempted to initiate multilateral mechanisms of their own. Second, private standard processes bring together a diverse community of high-profile experts who review and make recommendations on cyber norms for states and other stakeholders. Then, we have efforts from business to define cybersecurity standards which are referred to as industry-focused standard processes. The Microsoft-led Cybersecurity Tech Accord and the Siemens-led Charter of Trust are the two most influential examples of such mechanisms to date[220]. Finally, multistakeholder rule mechanisms are broad environments that provide opportunities for different players to address, define, or advance cyber norms, such as governments, international organisations, business, civil society, or academics. The multitude of sources of standards is not in itself bad and can even be beneficial because it takes into account a wider array of opinions. However, it creates a sub-optimal situation because the multitude of standards allows each states or stakeholders to choose a certain conference at the detriment of another because they feel this particular conference would best fit with their needs and interests. This raises concerns about *'forum shopping'*[221] as well as the possibility of division of norm initiatives where these systems compete or even contradict one another in their recommendations. This situation is therefore counterproductive and slows down Estonia in its quest for leadership in cybersecurity at the international level. Especially since it does not allow the stabilization and security of cyberspace.

[219] Duncan Hollis, 'Cyberspace and Geopolitics: Assessing Global Cybersecurity Norms processes at a Crossroads', (February 2020), https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110, accessed on April 30th, 2021

[220] SGS, 'The Charter of Trust takes a major step forward with cybersecurity', (February 2019), https://www.sgs.com/en/news/2019/02/the-charter-of-trust-takes-a-major-step-forward-with-cybersecurity, accessed on April 28th, 2021

[221] Ibid. 128

ii. The cybersecurity dilemma and the impossibility of stabilizing cyberspace

States will occasionally launch an attack to meddle into strategically sensitive networks of other states to ensure their own cybersecurity. However, those defensive attacks often involuntary threaten the other states' protection, causing escalation, and weakening global stability. The cybersecurity dilemma is the name given to this situation[222].

States will obtain vision into their potential adversaries' political leadership, consider their capacities, and conduct counterintelligence by penetrating each other's networks. In other words, infiltrating an adversary's computer systems will result in significant benefits for a state. Even a state that only wishes to build offensive options has a clear motivation to initiate intrusions ahead of time because a network attack can lead to significant damages. States will occasionally need, or believe they must, obtain intelligence in order to identify attacks more accurately and protect their own network. This information will help with cybersecurity. Recognizing this risk, states who discover an intrusion into strategically sensitive networks will feel threatened, even though the intrusion does not seem to have caused actual destruction. To mitigate this danger, states expend a lot of money and effort attempting to deter and track intrusions into their critical infrastructure[223]. As part of this defense initiative, any state will hack into the networks of other states to collect threat intelligence. As a result, intrusions can be motivated by defense goals.

The idea of the cybersecurity dilemma is inspired by the security dilemma, which is the long-held belief that states inadvertently and unintentionally instill distrust in other states as they seek to protect themselves. Consequently, other states are susceptible to act in attempt to reassert their own protection while unwittingly intimidating others and causing more escalation. Even if neither state wanted confrontation in the first place, the threat is present. However, unlike the security dilemma, the cyber security dilemma poses more of aproblems[224]. Indeed, most of what instinctively gives defenders advantages in traditional combat, such as the capacity to position stabilizing defensive fortifications at strategic chokepoints, has no apparent equivalents in cybersecurity. Similarly, distinguishing between defensive and offensive network intrusions is

[222] Ben Buchanan, 'The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations', (2017)

[223] Frédérick Douzet, 'Understanding cyberspace with geopolitics', (2014), https://www.cairn-int.info/article-E_HER_152_0003--understanding-cyberspace-with-geopolitic.htm, accessed on April 29th, 2021

[224] Wilson Center, 'The Cybersecurity Dilemma', (February 2017), https://www.wilsoncenter.org/event/the-cybersecurity-dilemma, accessed on April 30th, 2021

difficult, particularly since intrusions that begin as defensive in nature can easily morph to fit offensive goals.

The cybersecurity dilemma as well as the imminent strategic nature of cyberspace makes it very difficult to establish standards to regulate it. The impossibility of determining the nature of attacks forces states to be constantly on guard and therefore not to respect the established norms. There is thus the formation of a vicious circle of regulation. The absence of regulation leads to doubt in the states which cannot judge the nature of an attack. This doubt leads them to have offensive actions at each intrusion in their system. This behavior leads them to refutethe regulation of cyberspace which leaves them in doubt once again. Current cyber-security techniques are thus ineffective.

The state is at the forefront of this problem. On the one hand, state practices are evolving as a significant part of the issue, continuously causing more uncertainty and, in effect, impeding the elimination of identified insecurities. At the same time, without the intervention of the state, a free, stable, and open cyberspace is not feasible. So, how can we get out of this bind? Since it is a multi-state dilemma, answers cannot be sought exclusively by inter-state coordination[225]. Rather, an emphasis on a shared topic of concern for all parties involved in increased protection is advocated. If we want a safe and robust cyberspace, we must aggressively combat a strategically exploitable cyberspace full of vulnerabilities. This is a compromise that certain state actors must make if they want a form of national security that includes cyberspace. If such a solution is not reached, the pursuit of greater national security will still mean less cyber-security, which will always mean less national security due to weaknesses in sensitive infrastructure. This is where states can further strengthen cyber-security by enacting new regulations. But once again, we encounter the difficulty of regulating at the international level. It seems that the position of Estonia as a cyber norm entrepreneur on the international scene is more a myth than a reality.

iii. The United States' quest for leadership

Estonia has certainly been able to develop the image and instruments of a normative power in the field of cybersecurity at the international scale. However, it does not have the features of a great

[225] Myriam Dunn Cavelty, 'Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities', (April 2014)

power, meaning it does not have significant military and economic capacity, as well as political and soft power control, which can allow middle or small powers to weigh the great powers' views before taking their own measures. Estonia is not a great power in the sense of a politico-military entity capable comparable to the United States or China. It has therefore had to build a new form of power, with its current capabilities. Thanks to the European Union and NATO, it has strengthened what remains of its major political resource: its capacity to produce and implement, on a global scale, the broadest possible set of norms capable of organizing the world, disciplining the behaviour of its actors, introducing predictability into their behaviour, and developing in them a sense of collective responsibility. However, being a normative power is not simply being a power that resorts to the norm to act. Normative powers are limited to the norms. A normative power is a power that fundamentally has only the norm as a privileged, if not exclusive, instrument of international action[226]. This is why, the United States, as a superpower, is imposing itself de facto in the cyber space and is competing with Estonia in setting standards even though they share the same ideas.

The United States is one of the most Internet-dependent and attacked countries in the world. As an example, the 'cyber-commander' recently reported that these systems are attacked nearly six million times a day[227]. As early as 1998, President Bill Clinton signed Presidential Executive Order 63 on critical infrastructure protection, aimed at eliminating the vulnerabilities of their computer systems regarding cyber and physical attacks. In 2008, President George W. Bush approved Presidential National Security Directive 54, which formalizes a series of measures aimed at protecting government information systems against cyber-attacks. Finally, President Barack Obama invested heavily on the subject and made cybersecurity one of the priorities of his term. In a speech on May 29, 2009, he declared that *'the cyber threat is one of the most important economic and national security challenges that the United States faces.'*[228] In total, from 2010 to 2015, the U.S. government spent $50 billion on cyber defense, or about $10 billion per year, with several

[226] Zaki Laïdi, 'La puissance par la norme', (2008), https://www.cairn.info/la-norme-sans-la-force--9782724610888-page-63.htm, accessed on April 30th, 2021

[227] JDN, 'Le Pentagone attaqué 6 millions de fois par jours', (2010), https://www.journaldunet.com/solutions/dsi/1065095-zapping-de-la-securite-orange-pointe-du-doigt-le-pentagone-attaque/1065100-le-pentagone-attaque, accessed on April 29th, 2021

[228] The White House, 'Remarks by the President on Securing Our Nation's Cyber Infrastructure', (2009), https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure, accessed on April 29th, 2021

tens of thousands of officers working on these issues[229]. Cybersecurity became an increasingly important part of the U.S. defense and national security strategy. It is one of the top priorities of the National Security Strategy, published in 2010.

Because of its status as a great power, its soft power and its membership in NATO, the United States has influenced most European countries in the creation of cyber doctrines. Thus, without having a complete agenda to impose itself as a leader in cyber space, as Estonia was able to do, the United States has imposed itself de facto. Moreover, unlike Estonia, the U.S. authorities do not hesitate to state clearly that they reserve the right to respond by any means, including offensive capabilities, to a computer attack targeting the U.S. government, military, or economy[230]. The case of the United States shows that the norm is not enough to impose itself in a field as strategic as cyberspace. However, this is not in vain, some authors argue that the status of normative power is necessary as a basis on which to develop economic and military capabilities[231]. However, it is up to us to remain realistic, even if Estonia develops more characteristics of a great power, it is very unlikely that it could one day compete with the United States.

[229] Paul Cornish, 'On Cyber Warfare', (2010), https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf, accessed on April 30th, 2021

[230] Sénat, 'La cyberdéfense : un enjeu mondial, une priorité nationale', https://www.senat.fr/rap/r11-681/r11-68110.html, accessed on April 28th, 2021

[231] Ibid. 135

Chapter 2: Internal limits

In addition to Estonia's external limitations in cyberspace, there are also internal limitations that hinder its strategy as an international leader in cybersecurity. Many of the limitations were caused by initial advantages that may have been mismanaged. In addition, the lack of cybersecurity specialists hinders the development of new technologies and innovations. Finally, the flaws in the Estonian system call for even more vigilance and work to ensure a safe digital environment.

A) E-Estonia and the problem of innovation for innovation's sake

i. Financing nation branding on an alleged Russian threat

As we saw in the second part, Estonia has created a tailor-made image for itself, that of a state that is a forerunner in digital technologies and a promoter of global cybersecurity. However, despite all of its attempts to gain this prestige, Estonia's advances were easily caught up to, if not surpassed, by the advent of emerging innovations and the emergence of new areas in which certain countries had already differentiated themselves, mainly the United States, China and Russia. Maintaining a leading position on the international cyber and innovative scene has therefore very quickly become a priority for the country, for which cyber and emerging technologies in general remain the primary area in which it can differentiate itself at the European and international level.

Implementing a true digital nation-branding policy that includes cyber-defense, cybersecurity, and technology has emerged as a cure, or at the very least as a way to stay one step ahead[232]. This digital nation-branding is also embedded in Estonian institutions' perceptions of Russia as a challenge[233]. This historical threat justifies large expenditures in network security that may not be appropriate in the absence of an immediate danger. Even though Russia remains a danger due to its territorial proximity to Estonia, Russia's geopolitical and geostrategic ambitions have changed over the last ten years[234]. Estonia is no longer a primary target for Russia, despite

[232] Ibid. 35

[233] BTI, 'Estonia Country Report 2020', https://www.bti-project.org/en/reports/country-report-EST-2020.html, accessed on May 3rd, 2021

[234] Julia Gurganus, 'Russia's Global Ambitions in Perspective', (February 2019), https://carnegieendowment.org/2019/02/20/russia-s-global-ambitions-in-perspective-pub-78067, accessed on May 3rd, 2021

the central position that this idea still occupies in Estonian national cyber discourse to this day. Thus, information about impending potential threats in digital as well as physical space recurrently appears in Estonian media, coupled with news highlighting the success of Estonian organizations in defending the country's systems[235]. As a result, Russia is the main motif used by Estonia to promote its digital nation-branding campaign. However, this strategy is expensive and is undertaken by manipulating the population's view of the real threat posed by Russia.

ii. Media coverage pushing for the next major innovation

While media coverage has allowed Estonian to make itself known, it has also been to its detriment. Indeed, the media frenzy that has served Estonia so well could be negative in the long run. The country is expected to be on the verge of its next massive innovation, either in digital or security terms, but it still doesn't seem to know where to look.

Any emerging technology, such as blockchain, bitcoin, and artificial intelligence, have piqued the interest of several people. Artificial intelligence already helped Estonia make international headlines in early 2019, as the country decided to develop legal artificial intelligence to autonomously adjudicate minor lawsuit cases to ease the workload of judges[236]. This announcement stimulated the interest, or perhaps alarmed, people around the world. However, upon closer inspection, this is nothing new for the country. Since 2017, artificial intelligence has been at the disposal of the Estonian government, and it now runs more than thirteen separate schemes, such as the automatic registration of children with a public school at birth[237].

In the case of Estonia, which is undergoing significant population decline due to its low birth rate, some use cases of artificial intelligence, be it school registration or court rulings, can easily be justified and allow for the improvement of government programs rendered in order to strengthen and promote the lives of its people. Aside from improving government services, Estonia's choices for staying in the media spotlight are unsuitable to the needs of the people, posing the question of whether change is sought for its own sake or for the sake of national welfare.[238].

[235] Ibid. 35

[236] Eric Niller, 'Can AI be a fair judge in court? Estonia thinks so', (March 2019), https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/, accessed on May 3rd, 2021

[237] E-Estonia, 'Estonia accelerates artificial intelligence development', (May 2019), https://e-estonia.com/estonia-accelerates-artificial-intelligence/, accessed on May 3rd, 2021

[238] Ibid. 35

Whether it's artificial intelligence or cryptocurrencies, innovation for the sake of innovation may result in much more problems than solutions. While these systems are relatively new, they are also far from flawless and can cause security or organizational issues. Despite their level of maturity, they are vulnerable to future computer attacks. The main risk of relying on these technologies for Estonia is that it would monopolize the country's already insufficient labour force to build and protect these early-stage technologies, rather than waiting until they are mature and secure to use in innovative ways. Thus, the quest for the next step to take for Estonia to retain its position as a leader in innovation and emerging technology could prove risky in the long run, undermining the evolution of pre-existing processes, mechanisms, and applications.

The introduction of digital nation-branding policies seems to have hampered the advancement of emerging technology, forcing the country to keep ahead of foreign innovation rather than inventing what it requires in order to retain its voice and reputation as an authority in the field. This dichotomy is mirrored in the evolution of Estonian digital democracy, where civil society is still trying to find its position. Citizens, despite using these services on a regular basis, remain for the time being consumers rather than actors, contrary to what the word e-democracy suggests.

iii. The need for innovation in the cybersecurity sector

It seems that Estonia is staying ahead of the curve more in the digital sector more so, than in cybersecurity. Indeed, technology, combined with a demand for territorial independence and digital sovereignty, has resulted in some significant developments and novel uses of digital space. The establishment of an Estonian e-embassy in Luxembourg in 2017, with the aim of shielding government data from possible Russian territorial incursion, was undertaken not for international outreach, but to virtually shield the country as a whole[239]. This embassy hosts a backup of the digital government data to ensure the stability of Estonian digital services, keeping them available even though national networks are completely shut down or damaged. The dematerialization of Estonia's territories via its e-ambassy, which is deemed by law to be an inviolable territory ruled by Estonian law leads to a reterritorialization of Estonia outside its boundaries via technology. This project was necessary to respond to a required need for data protection. On the other hand,

[239] OECD, 'Case Study: the world's first data embassy', (2017), https://www.oecd.org/gov/innovative-government/Estonia-case-study-UAE-report-2018.pdf, accessed on May 3rd, 2021

the establishment of the status of e-citizen enables everyone in the world to apply for Estonian e-residency and thereby gain access to its online facilities. This innovation in the use of digital technology, more than in the technology itself, has allowed the country to revitalize itself in terms of population but also in terms of image, seeking now to attract new generations of entrepreneurs to keep its reputation as a young and innovative country. Through these two initiatives, among which e-citizenship will have required only a few means for its deployment, Estonian digital democracy has continued its growth by using digital space as a space in its own right, and by renewing the traditional perception and definition of national space and territory, as well as that of citizenship and belonging to a State. However, to be a leader not only in digital democracy but also in cybersecurity, Estonia should re-allocate its resources and efforts in an equitable way so as not to lose its lead in digital technology and continue its innovations in cybersecurity. It could continue to develop ideas in terms of encryption, which it is already doing with its digital identity cards.

B) The lack of cybersecurity professionals

The advances that have propelled Estonia to the forefront of the digital sector are reaching their limits, owing primarily to a shortage of cybersecurity and technology specialists[240]. There are now too many areas to protect due to the nation branding strategy but not enough professionals to do so. Estonia tried to counter the lack of workers in the fields of cybersecurity and new technologies by resorting to two very effective but no longer sufficient methods.

First, Estonia achieved outstanding results in addressing the shortage by implementing effective educational policies. For instance, the ProgeTiger initiative and the Unicorn Squad for girls aged 8 to 12[241] were very successful but now, the Education and Youth Board, HARNO, is up against schools opposed to the technologization of education on the one side, and a shortage of skills among teaching staff to use and teach new technologies on the other[242]. If the teaching provided to the youngest is primarily aimed at teaching them the automatisms and reasoning

[240] Ibid. 35

[241] Education Estonia, 'How Estonia is solving the shortage of ICT specialist?', (March 2021), https://www.educationestonia.org/how-estonia-the-pisa-leader-is-solving-the-shortage-of-ict-specialists/, accessed on May 4th, 2021

[242] Education and Youth Board, 'The challenges', (June 2020), https://harno.ee/en, accessed on May 4th, 2021

needed to begin programming later in life, the teaching of emerging technology in secondary schools remains the key issue confronting Estonian digital nation-branding[243]. Indeed, primary school education is mostly focused on basic programming languages or non-digital programming techniques that are easily accessible to teachers with no programming or robotics experience. At the secondary level, though, a shortage of instructors capable of teaching these subjects at a higher level often leads to class interruptions and, as a result, a loss of expertise for students who have been trained for many years and must thus start from scratch as they wish to pursue technical studies in higher education.

The shortage of trained experts in the fields of digital technologies and cybersecurity is also becoming a serious issue. Professor at Tallinn University of Technology, TalTech, Rain Ottis said that the sector was growing faster than the number of graduated students even though the university has launched a higher education program in cybersecurity and computer science. The dropout rate for computer science and new technology students remains among the highest in the country[244]. Furthermore, since it is surrounded by countries with far higher wages than its own, Estonia is experiencing a brain drain to Finland, Sweden, Norway, Denmark, or Germany, where specialists educated in its universities are chasing salaries that are double or triple those paid on its territory[245]. The recruiting of specialists within private companies engaged in growth and invention in collaboration with the government and the key Estonian research centers is becoming extremely difficult, especially because the latter are in direct competition with the army. Estonia is therefore lacking cybersecurity experts needed to protect the country, which is concerning given the current and increasingly advanced cyber-threats.

Temporary alternatives have been sought, such as the army integrating computer-savvy conscripts into the Signal Battalion under the authority of the Cyber Command[246]. In the long run, however, the global race to innovate risks to undermine structures that are already weakened by a lack of manpower and the departure of Estonian specialists seeking better incomes abroad, forcing those who remain in Estonia to constantly train in subjects that are often well removed from their

[243] Education Estonia, ‘Phenomenon based Learning in Finland & Programming in Estonian Schools and Kindergartens’, (January 2021), https://www.youtube.com/watch?v=gJ6SS65q_lg, accessed on May 4th, 2021

[244] Ibid. 35

[245] The Global Economy, ‘Estonia: human flight and brain drain’, https://www.theglobaleconomy.com/Estonia/human_flight_brain_drain_index/, accessed on May 4th, 2021

[246] Republic of Estonia Defence Forces, ‘Cyber Command’, https://mil.ee/en/landforces/cyber-command/, accessed on May 4th, 2021

professional skills in order for the country to continue to distinguish itself on the international scene.

The second method used by Estonia is the voluntary Cyber Defence Unit made up of ordinary people who are professionals in crucial cyber-security roles outside of government, patriotic persons with information technology experience, and experts in other sectors who choose to volunteer outside of their regular careers to defend Estonian cyberspace. However, this solution, once again, is no longer sufficient to counter the growing number of cyber-threats. To maintain its role in cyberspace, Estonia will therefore need to solve this skilled labor problem by training more teachers, implementing public policies to make cybersecurity jobs more attractive in Estonia than in neighboring countries and advocating common European policies to tackle brain drain in a joint effort.

C) A system with exploitable flaws

i. Network attacks in 2019

First and foremost, the Covid19 pandemic showed that Estonia was still very dependent on the internet, and something had to be done to better protect the medical sector. However, for this part we will rely on the yearbook published in 2020 by the Estonian Information System Authority, RIA, which traces the events that occurred in 2019 in cyberspace[247]. The Analysis and Prevention Department of the RIA's Cybersecurity Directorate analyzes patterns in Estonian cyberspace and focused largely on CERT-EE occurrences. Based on the input collected, the department creates reports. This is the most recent data we have found. According to the alerts issued by RIA's incident response department, CERT-EE, 2019 is the year of phishing. While infections of robotic networks are the source of most alerts, the amount of infections Estonian authorities were aware of has declined, whilst the number of phishing pages and phishing attacks has nearly doubled.

Before 2019, cybercriminals whose primary goal is to steal money from banks have largely avoided targeting Estonians. This is most likely because Estonian banks use reasonably stable

[247] Republic of Estonia Information System Authority, ‘The 2020 Yearbook of the Information System Authority’, (2020), https://www.ria.ee/sites/default/files/content-editors/ria_aastaraamat_2020_48lk_eng.pdf, accessed on May 5th, 2021

authentication mechanisms such as ID cards, Mobile-ID, and Smart-ID[248]. However, in April 2019, attackers discovered a way to build new Smart-ID accounts in the names of their victims by using phishing messages and websites[249]. The offenders sent a message to the user's mobile phone on behalf of the bank, claiming to be a link to the bank's login page. The victim was then asked to log in using their Mobile-ID. The offenders began developing a new Smart-ID account around the same time they entered their username, personal identity code, and PIN1 on the phishing platform. After opening the account under the victim's name, the suspects signed into the bank and moved the funds. Besides phishing letters and webpages designed to steal money, phishing efforts based on stolen account data have caused significant harm[250]. A quick email advising users that their mailbox is overflowing or requesting that they update their password will provide hackers with easy access to their personal messages as well as the opportunity to distribute their phishing emails more broadly.

RIA has seen many cases of phishing scams in 2019 that should have been avoided with multi-level authentication. Local government employees, at least three of Estonia's major colleges, hospitals, and smaller establishments such as a gasoline company and a road repair company were all victims of this form of phishing[251]. Trying to eliminate the implications of breaches and assessing the scope of information leakage is often hampered by the fact that information management departments, or service providers lack adequate logs to establish which email addresses have been hacked and to what degree. A good log management system is required if the authority is to determine what kind of information has been compromised.

Furthermore, in 2019, RIA recorded enormous service interruptions that may have had a significant effect on the Estonian population. In September, a software error rendered the Emergency Response Center phones offline for 20 minutes, in November, the Digital Order and the state portal were unavailable for hours due to an unforeseen break in state network cables, and in December, the Digital Order was ineffective once more. In May, the migration of Mobile-ID to new systems disrupted this authentication and signature process for 24 hours, the community register, national authentication service, new version of X-tee, and other services had also

[248] E-Estonia, ‘e-identity’, https://e-estonia.com/solutions/e-identity/smart-id/, accessed on May 5th, 2021
[249] ERR, ‘RIA: New type of financial fraud spreading in Estonia’, (February 2021), https://news.err.ee/1055523/ria-new-type-of-financial-fraud-spreading-in-estonia, accessed on May 5th, 2021
[250] Ibid. 156
[251] RIA, ‘Annual Cyber Security Assessment 2019’, (2020), https://www.ria.ee/sites/default/files/content-editors/kuberturve/ktt_aastaraport_eng_web.pdf, accessed on May 5th, 2021

crashed[252]. Estonians are so accustomed to digital services that Estonian administrations must invest in their availability, ensure operational stability, test processes, develop practices, and test again. In 2019, service outages were mostly caused by human error, administrative error, or natural causes, but fragile networks can often malfunction as a result of malicious people and attacks. The Avalanche botnet[253], for example, was responsible for several of the malware incidents recorded in 2019. It was shut down in December 2016 after a multinational law enforcement action, but malware does not immediately vanish from networks, and they must be cleaned up separately to prevent the same infrastructure from being taken over later. Most of the compromised computers joined the Necurs botnet[254], which has been used for years to carry out denial-of-service attacks, ransomware delivery, spamming, and other malicious activities. Microsoft disclosed in March 2020 that it had gained control of the network. Nonetheless, many infected devices remain in Estonia, though they are no longer as dangerous to others. There are also a number of computers in Estonia that have joined another botnet. Without their owners' awareness, Internet of Things devices whose software has not been upgraded or whose system configuration password has not been changed will join those networks and deliver the same phishing or malware messages that caused so many problems last year.

Estonia, despite all the measures it has put in place after 2007 to fight against attacks in cyberspace and make it safer for its citizens, is still subject to numerous attacks. This fact represents an internal limit to its success on the international scene and therefore calls for concrete measures to prevent them.

ii. RIA's actions to reduce insecurities in cyberspace

In order to increase awareness among the Estonian people, RIA organised information campaigns. This began a few years ago with the Vaata Maailma Foundation's Nuti-Mati initiative, which raised awareness about the protection of smart devices[255]. However, the time has now come for the RIA to examine intelligence operations more thoroughly, by using survey data from Statistics Estonia, Eurostat, and other sources to help identify target audiences for awareness campaigns. The study

[252] Ibid. 160
[253] **Glossary**
[254] **Glossary**
[255] Ibid. 156

specifically identified a population with low cyber hygiene, but which has received less attention when it comes to cybersecurity: seniors[256].

Over the years, the Estonian Union for Child Welfare, the Police and Border Guard Board, and other ministries, for example, have paid close attention to young Internet users. Older people, on the other hand, have had to adapt and fight for themselves in a changing cyberspace. As a result, in the second half of 2019, the RIA organized a major awareness campaign on basic cyber hygiene skills, with the population aged 55 and up as the primary focus group. RIA also collaborated with the Estonian Librarians Association during the initiative. On the November information day, people from all over Estonia had the chance to visit their public library for cybersecurity information. The campaign communications reached at least 80% of the target demographic through advertisement and public relations programs[257]. According to the follow-up poll, more than a quarter of people who saw the campaign advertisements took at least one step to improve their own online protection. The aim was to use the initiative to highlight the importance of safety to older adults on the one hand, and to inspire the public to help their older peers and relatives act more responsibly in cyberspace on the other.

RIA agreed to extend this program in 2020, focusing on small and medium-sized enterprises, which are the most vulnerable to service disruptions, ransomware, and financial fraud from compromised email addresses. The more company leaders are aware of possible cyber-attacks, the better equipped they would be to delegate their IT services and shield their companies from cyber threats. These two examples contribute to a deeper understanding of how RIA can deter high-impact cyber accidents in Estonia.

Besides, as wellness, security and vital services become more reliant on information technology, RIA must prioritize reliability and protection. Events in Ukraine in 2015, which left people without power in December, and in the United Kingdom, where the National Health Service had to postpone thousands of hospital appointments due to WannaCry, have shown that an assault on IT processes can have a rapid and devastating impact on the real world[258]. The RIA conducts the defense of critical information infrastructures, which includes preparing risk analysis of

[256] Statistics Estonia, 'The statistical council reviewed last year and was briefed on census methodology', (February 2021), https://www.stat.ee/en/uudised/statistikanoukogu-tegi-aastast-kokkuvotte-ja-vottis-teadmiseks-rahvaloenduse-meetodi, accessed on May 6th, 2021

[257] Ibid. 160

[258] BBC News, 'Ukraine power-cut was a cyber-attack', (January 2017), https://www.bbc.com/news/technology-38573074, accessed on May 6th, 2021

emergency situations triggered by cyber-attacks, developing appropriate compliance procedures, organizing security checks, and providing disaster management and response guidance to important and crucial service providers[259]. Under the guidance of the RIA, emergency risk evaluations for major cyber accidents are planned on a daily basis. They measure the risk and implications of an emergency and identify the action that must be taken to avert an emergency or, if prevention is not possible, to minimize the consequences.

In addition to educating actors and providing assistance, RIA engages in simulation exercises to better prepare for incidents in cyber space. As such, in March 2019, Estonians and their Finnish counterparts practiced resolving a malware threat against energy providers. RIA also organized Estonia's role in Locked Shields, the world's largest multinational cyber security drill, in April[260]. They assisted in the preparation for and participation in the NATO crisis management exercise, which involved cyber threats, in May. In December, they assisted in the organization of the NATO Cyber Coalition 2019 cyber security exercise in Tartu[261]. Furthermore, RIA organized annual exercises in which civil and military forces worked together to tackle a cyber incident. The more complicated the simulations, the faster it would be to handle a real-life problem. Estonia has internal limits, but it seems that it has the capacity to overcome them.

[259] RIA, 'Cyber Security in Estonia in 2020', https://www.ria.ee/sites/default/files/content-editors/RIA/cyber_security_in_estonia_2020_0.pdf, accessed on May 6th, 2021

[260] CCDCOE, 'Locked Shields', https://www.ria.ee/sites/default/files/content-editors/RIA/cyber_security_in_estonia_2020_0.pdf, accessed on May 6th, 2021

[261] Cyber Command, 'NATO Cyber defence exercise', https://www.cybercommand.ro/app/webroot/en/press_releases/view/2, accessed on May 6th, 2021

CONCLUSION

The purpose of this paper was to demonstrate that the 2007 cyber-attacks against Estonia transformed its role on the international scene and that the country was able to take advantage of these attacks to build a new reputation as an entrepreneur of cyber norms. In other words, 'Estonia seized the opportunity to be a speaker for cyber'[262].

As we've seen, the DoS and DDoS attacks that hit Estonia for many weeks in the spring of 2007 elicited a wide range of response. One of the most perplexing contradictions was the difference in perceptions between Estonian politicians and the Estonian people. The first ones labeled the operations the *'first cyber war'*, despite the fact that a large portion of the people were unaware of the attacks and were unconcerned. Moreover, the political class was open with the public and the international community, referring to the activities as cyber-attacks. This transparency allowed the authorities to call for international assistance and put Estonia in the spotlight. As a result, the attacks prompted reactions outside of Estonia, particularly among NATO, the United States, and the European Union, which have become fearful and acutely aware of the strategic importance of cyberspace. For instance, the US and NATO dispatched technical assistance and specialists to the site, while the European Union, in a more ethical stance, condemned Russia's action. Finally, Russia, the main accused, simply denied responsibility for the cyberattacks and called on its citizens to boycott Estonian products.

These attacks have brought the cyber issue to the forefront of the international community's discussion and demonstrated Estonia's resilience, which has been able to recover owing to legislative and socio-cultural improvements, but most notably thanks to new and more effective cyber defense mechanisms. They have, however, shown the shortcomings of international law in the attribution of cyber-attacks. As a result, Estonia has used this gap to carve out a new role for itself as a cyber norms entrepreneur. This shaping was made possible, first and foremost, thanks to Estonia's nation branding strategy, which intended to establish the country's reputation as a cybersecurity pioneer. President Ilves has also played an important role in promoting Estonian values and making Estonia renowned on a global scale. These efforts culminated in the publication of two versions of the Tallinn manual, which address worldwide cyber security challenges and, most all, demonstrate NATO's support for Estonia, which is critical for a small country.

[262] Interview with Professor Rain Ottis

With the establishment of this role, Estonia has been able to disseminate its values on a global scale through numerous organizations. NATO was able to increase its cyber capabilities and build a cyber strategy as a result of this dissemination. The EU has also developed a cyber diplomacy and is the driving force behind the EU CyberNet Initiative. Finally, Estonia has pushed the cyber problem to the United Nations through the UNGGE and OEWG. Estonia has therefore used the attacks to establish itself as a trusted ally on the world stage, as well as a pioneer in cyber security. This case is significant because it highlights the necessity of alliances for small states like Estonia, a former Soviet Union republic that has been able to grow and carve out a distinct space for itself on the world stage. On the other hand, it demonstrates the importance of more advanced international cooperation.

Furthermore, as we have seen, Estonia's case has certain limitations, not only because it has a hostile neighbor that does not aim to align itself with international cyber principles, but also because it faces a lack of unanimity within its own camp in the west. Additionally, Estonia appears to be caught up in a frenzied race for innovation, which may backfire because innovations are generated for worldwide impact rather than for the benefit of its society. It also has a scarcity of cyber professionals and, despite its efforts, remains vulnerable to cyber-attacks. So, what are its prospects in cyberspace and the international community? One approach would be to first push outside the boundaries we've established, and then to carve out a niche in which Estonia would be the undisputed leader. This is something it will continue to do, as indicated by its chair of the United Nations Security Council in June 2021. During its presidency, Estonia will make cybersecurity an issue at the UNSC meetings[263]. However, Professor Ottis noted that what brought Estonia to where it is now, might not bring Estonia further and that the country should take care of the legacy past successes brought. On the other hand, it should not lose sight of the need of aligning its international and national interests and that cybersecurity is not important if there is nothing to secure. So, more than waiting for the next big bang that artificial intelligence might bring, Estonia should find ways to conduct digital life in a more secure manner. Finally, the Estonian experience exposes the wider issue of international agreement on cyber norms.

[263] Interview with EU CyberNet Director, Siim Alatalu

Appendix, Glossary and References

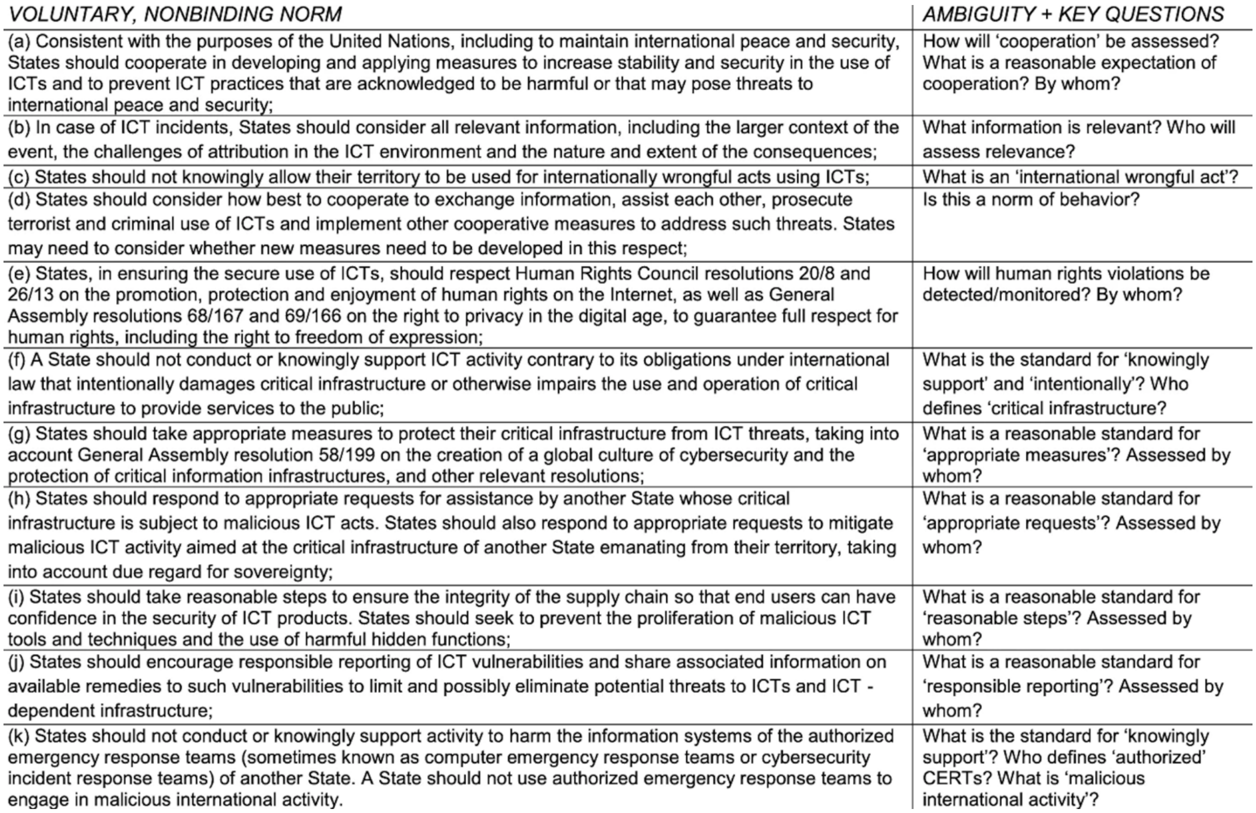
Appendix 1: Interviews

Joshua Gold, Visiting Fellow at the Canadian International Council, focuses on various topics in international relations, global affairs, and security – particularly issues related to global cyberspace governance, conflict in cyberspace, and internet governance.

Rain Ottis, Professor of cyber security in Tallinn University of Technology. During 2008-2012, was a scientist / senior analyst with the NATO Cooperative Cyber Defence Centre of Excellence, Estonia. While there, focused on alternative setups of cyber forces and national cyber security topics.

Siim Alatalu, Director of EU CyberNet, joined the NATO Cooperative Cyber Defence Centre of Excellence in January 2015. In 2018 he joined the Centre's Strategy Branch, overseeing cyber strategy and policy research and training related to NATO and the European Union, as well as providing subject matter expertise to the Centre's other flagship projects. His previous career has been with the Estonian Ministry of Defence, also including a diplomatic assignment at the Estonian Delegation to NATO in Brussels, Belgium. During the Estonian Presidency of the Council of the European Union in 2017, he also co-led the development of EU's cyber policy and strategy, being the Vice Chair of the Council's Horizontal Working Party for Cyber Issues.

Appendix 2: 2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law



VOLUNTARY, NONBINDING NORM	*AMBIGUITY + KEY QUESTIONS*
(a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;	How will 'cooperation' be assessed? What is a reasonable expectation of cooperation? By whom?
(b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;	What information is relevant? Who will assess relevance?
(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;	What is an 'international wrongful act'?
(d) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;	Is this a norm of behavior?
(e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;	How will human rights violations be detected/monitored? By whom?
(f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;	What is the standard for 'knowingly support' and 'intentionally'? Who defines 'critical infrastructure?
(g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;	What is a reasonable standard for 'appropriate measures'? Assessed by whom?
(h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;	What is a reasonable standard for 'appropriate requests'? Assessed by whom?
(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;	What is a reasonable standard for 'reasonable steps'? Assessed by whom?
(j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT - dependent infrastructure;	What is a reasonable standard for 'responsible reporting'? Assessed by whom?
(k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.	What is the standard for 'knowingly support'? Who defines 'authorized' CERTs? What is 'malicious international activity'?

https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/

Glossary

Avalanche: a criminal organization that carried out phishing attacks, online bank theft, and ransomware. The term also applies to the network of owned, licensed, and corrupted systems that is used to carry out the operation. Only computers running the Microsoft Windows operating system became infected by Avalanche. After a four-year effort by a multinational group of law enforcement, commercial, research, and private organisations, the Avalanche botnet was dismantled in November 2016.

Botnet: formed from the two words ‘robot’ and ‘network’, it is a network of hijacked computers and devices infected with bot malware and remotely controlled by a hacker. It is used to launch DDoS attacks.

Cloud: all the hardware and software accessible via the Internet, which a service provider makes available to its customers in the form of online services.

Critical Infrastructure: a system that is critical for the preservation of fundamental societal functions, as well as people's health, safety, security, economic, or social well-being, and whose interruption or destruction would have a major impact on a State as a result of failing to maintain such functions.

Denial of Service attacks: (DoS attacks): attack meant to shut down a machine or a network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic.

Necurs: botnet that distributes a wide range of malware.

Ping Flood: common Denial of Service attack in which the attacker takes down a victim’s computer by overwhelming it with request packets, also known as pings, to which the network will respond with an equal number of reply packets.

Trojan Virus: type of malware that is disguised as legitimate software. It is used to gain access to user's systems.

X-Road: software and pillar of e-Estonia. It allows the nation's various public and private sector e-service information systems to link up and function in harmony. It ensures secure transfers by encrypting and logging data.

References

- Aronczyk, Melissa. *How to Do Things with Brands: Uses of National Identity.*

- Barat-Ginies, Oriane. *Existe-t-il un droit international du cyberespace ?* Accessed on April 7th, 2021. https://www.cairn.info/revue-herodote-2014-1-page-201.htm

- Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*.

- Connell, Michael. Russia's Approach to Cyber Warfare. accessed on April 26th, 2021. https://apps.dtic.mil/dtic/tr/fulltext/u2/1019062.pdf

- Cooperative Cyber Defence Centre of Excellence. *Tallinn Manual Process*. Accessed on April 6th, 2021. https://ccdcoe.org/research/tallinn-manual/

- Crandall, Mathew, Allan, Collin. *Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms.* Accessed on March 14th, 2021. https://www.tandfonline.com/doi/abs/10.1080/13523260.2015.1061765?journalCode=fcsp20,

- Davis, Joshua. *Hackers take down the most wired country in Europe*. Accessed on March 15th. 2021. https://www.wired.com/2007/08/ff-estonia/

- De Pommereau, Isabelle. *Estonia reaches out its ethnic Russians at long last*. Accessed March 15th, 2021. https://www.dw.com/en/estonia-reaches-out-to-its-ethnic-russians-at-long-last/a-42680725

- Deschaux-Dutard, Delphine. *L'Union européenne : une cyber puissance en devenir ? Réflexions sur la cyber défense européenne.* accessed on April 20th, 2021. https://www-cairn-info.scd-rproxy.u-strasbg.fr/revue-internationale-et-strategique-2020-1-page-18.htm#no8

- ENISA. *Cyber Security Strategy*. Accessed on May 25th, 2021

- ENISA. *2014-2017 Cyber Security Strategy*. Accessed on May 26th, 2021 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf

- Evron, Gadi. *Battling Botnets and Online Mobs: Estonia's Defense Efforts During the internet War*. Georgetown Journal of International Affairs

- Finn, Peter. *Cyber Assaults on Estonia Typify a New Battle Tactic*. Accessed March 16th, 2021. https://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html

- Finnemore, Martha, Sikkink, Kathryn. *International Norm Dynamics and Political Change*. Accessed on April 10th, 2021. https://www.jstor.org/stable/2601361?seq=1

- Gold, Josh. Estonia as an international cybersecurity leader. Accessed on April 2nd, 2021. https://e-estonia.com/estonia-as-an-international-cybersecurity-leader/

- Goldstein, Jeff. *Estonia's Cyber Attacks: Lessons Learned.* Accessed March 15th, 2021. https://wikileaks.org/plusd/cables/07TALLINN375_a.html

- Haataja, Samuli. *Cyber-attacks and international law on the use of force,* chapter 5 'The 2007 cyberattacks against Estonia' (2018)

- Herzog, Stephen. *Revisiting the Estonian Cyber Attacks: Digital threats and Multinational Responses*. Journal of Strategic Security (Summer 2011)

- Herzog, Stephen. *Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity.* Accessed on May 25th, 2021. https://www.researchgate.net/publication/326986589_Ten_Years_after_the_Estonian_Cyberattacks_Defense_and_Adaptation_in_the_Age_of_Digital_Insecurity

- ICDS. *Russia involvement in the Tallin Disturbances*, Accessed March 15th, 2021. https://icds.ee/en/russias-involvement-in-the-tallinn-disturbances/

- Ilves, Toomas H. *Address by the President of Estonia*. Accessed March 15th, 2021. https://vp2006-2016.president.ee/en/official-duties/speeches/7991-address-by-h-e-toomas-hendrik-ilves-president-of-estonia-to-the-67th-session-of-the-united-nations-general-assembly-un-headquarters-new-york-september-2012/

- Kaisa, Saarenmaa. The Tiger Leap – Information society in Estonian frames. Accessed on March 15th, 2021. https://longterm.softf1.com/2018/blog_resources/2002_xx_xx_The_Tiger_Leap_Information_Society_in_Estonian_Frames_by_Kaisa_Saarenmaa_and_Osma_Suominen_keywords_history_education_Internet_network_computers.pdf

- Kaska, Kadri. The Cyber Defence Unit of the Estonian Defence League. Accessed on April 12th, 2021. https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf

- Keary, Tim. *DoS vs DDoS Attacks: The Differences and How To Prevent Them*. Accessed March 16th, 2021. https://www.comparitech.com/net-admin/dos-vs-ddos-attacks-differences-prevention/

- Lambeth, Benjamin. *Operation Allied Force: Lessons for the Future*. accessed on April 19th, 2021. https://www.rand.org/pubs/research_briefs/RB75.html

- Leetaru, Kalev. What Tallinn Manual 2.0 Teaches Us About the New Cyber Order. Accessed on April 7th, 2021. https://www.forbes.com/sites/kalevleetaru/2017/02/09/what-tallinn-manual-2-0-teaches-us-about-the-new-cyber-order/

- Li, Sheng. *When does Internet Denial Trigger the Right of Armed Self-Defense?* (2013). Yale Journal of International Law

- Limonier, Kévin. *La Russie dans le cyberespace: représentations et enjeux.* Accessed on April 26th, 2021. https://www.cairn.info/revue-herodote-2014-1-page-140.htm

- Magnusson, Jakob. *The question of preventing cybercrime against governmental institutions*. accessed on April 7th, 2021. https://www.unodc.org/unodc/index.html

- Mälksoo, Lauri. The Tallinn Manual as an international event. Accessed on April 5th, 2021. https://icds.ee/en/the-tallinn-manual-as-an-international-event/

- Markoff, John. Before the Gunfire, Cyberattacks. Accessed on April 15th, 2021. https://www.nytimes.com/2008/08/13/technology/13cyber.html

- Ministry of Economic Affairs and Communication. *2014-2017: Cyber Security Strategy*. Accessed on April 1st, 2021. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf

- NATO CCDCOE. *2007 cyberattacks on Estonia*

- NATO. *Strategic Concept for the Defence and Security of the members of the North Atlantic Treaty Organization*. accessed on April 19th, 2021. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

- NATO. *Wales Summit Declaration.* Accessed on April 11th, 2021. https://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease

- Nazario, Jose. *Estonian DDoS Attacks – A Summary to Date*. Accessed March 16th, 2021. https://www.netscout.com/arbor-ddos

- Ottis, Rain. Analysis of the 2007 Cyber-attacks against Estonia from the information warfare perspective. Accessed March 15th, 2021. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

- Republic of Estonia Information System Authority. *State information system in Estonia.* Accessed on March 16th, 2021.https://www.ria.ee

- Republic of Estonia Information System Authority. *The 2020 Yearbook of the Information System Authority.* Accessed on May 5th, 2021.https://www.ria.ee/sites/default/files/content-editors/ria_aastaraamat_2020_48lk_eng.pdf, accessed on May 5th, 2021

- RIA. *Annual Cyber Security Assessment 2019'*. accessed on May 5th, 2021. https://www.ria.ee/sites/default/files/content-editors/kuberturve/ktt_aastaraport_eng_web.pdf

- RIA. *2019-2022 Cyber Security Strategy.* Accessed on May 26th, 2021. https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

- Riigi Teataja. *Cyber Security Act*. Accessed on May 26th, 2021.https://www.riigiteataja.ee/en/eli/523052018003/consolide

- Risse, Thomas. *International human rights norms and domestic change: conclusions*. Accessed on April 11th, 2021. https://www.cambridge.org/core/books/power-of-human-rights/international-human-rights-norms-and-domestic-change-conclusions/6822537228C126F25EE1B2332BCF9FD5

- RKK ICDS. *How Estonia uses Cybersecurity to Strengthen its Position in NATO*. Accessed on April 19th, 2021. https://icds.ee/en/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/

- Ronzaud, Léa. *E-Estonie" : le "nation-branding" numérique comme stratégie rayonnement international.* Accessed on April 12th, 2021 https://www.cairn.info/revue-herodote-2020-2-page-267.htm

- Schmitt, Michael. *The Tallinn Manual 2.0 on the International Law of Cyber Operations.* Accessed on April 5th, 2021. https://www-cambridge-org.myaccess.library.utoronto.ca/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9

- Schmitt, Michael. *The Tallinn Manual 2.0 on the International Law of Cyber Warfare.* Accessed on April 5th, 2021. https://www-cambridge-org.myaccess.library.utoronto.ca/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE

- Schmitt, Michael. *The Tallinn Manual 2.0 on the International Law of Cyber Operations: What it is and isn't*. Accessed on April 5th, 2021. https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/

- Talbot Jensen, Eric. The Tallinn Manual 2.0: Highlights and Insights. Accessed on April 6th, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2932110

- Tamkin, Emily. *10 Years after the landmark attack on Estonia is the world better prepared for Cyber threats?* Accessed March 16th, 2021.

https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

- Tapon, Francis. *The Bronze Soldier explains why Estonia prepares for a Russian cyberattack*. Accessed March 15th, 2021. https://www.forbes.com/sites/francistapon/2018/07/07/the-bronze-soldier-statue-in-tallinn-estonia-give-baltic-headaches/

- TheCyberDiplomat. *Tallinn Manual – A Brief Review of the International Law Applicable to Cyber Operations*. Accessed on April 5th, 2021. https://medium.com/@cyberdiplomacy/tallinn-manual-a-brief-review-of-the-international-law-applicable-to-cyber-operations-5643c886d9e2

- Traynor, Ian. *EU Protests over Russians Attacks on Ambassadors*. Accessed March 15th, 2021. https://www.theguardian.com/world/2007/may/03/russia.eu

- Traynor, Ian. *Russia accused of unleashing cyberwar to disable Estonia*, The Guardian. Accessed March 15th, 2021. https://www.theguardian.com/world/2007/may/17/topstories3.russia

- Tuohy, Emmet. Towards an EU Cybersecurity Strategy: the Role of Estonia. accessed on April 20th, 2021. http://pdc.ceu.hu/archive/00006852/01/ICDS_Toward-EU-Cybersecurity-Strategy-The-Role-of-Estonia.pdf

- University of Reading. *Michael Schmitt.* Accessed on April 5th, 2021. https://www.reading.ac.uk/law/Staff/m-schmitt.aspx

- Wiseman, Geoffrey. *Diplomacy in a globalizing world: theories and practices*.