EXPLORING POLICY CONDITIONS FOR CYBER DETERRENCE: A CASE STUDY OF ESTONIA

LIONEL OH¹

ABSTRACT

This article seeks to study the policy conditions for the successful application of deterrence theory in cyberspace. While the tenets of classical deterrence theory are difficult to apply to cyberspace, understanding the applicability of these concepts in the cyber context is crucial as cyberspace continues to transform into a prominent domain of conflict. Classical deterrence has always been closely associated with a Cold War-era nuclear context, and its translation to cyberspace will require a broader approach to account for changes in the nature of the domain. The success of Estonia's multi-faceted deterrence efforts after experiencing a large-scale cyber-attack in 2007 shows the effectiveness of such a conception of deterrence to the realm of cyberspace, through the implementation of international and domestic level policies. I analyze how Estonia has managed to implement this deterrence framework by punishment, denial, multilateral cooperation and promotion of international norms, and an increase in societal strength and resilience among its population.

¹ Lionel Oh is a sophomore at Tufts University studying International Relations and Computer Science. An avid believer in public service with a strong interest in anything related to defense, he serves as a military officer with the Republic of Singapore Air Force. At Tufts, he is a member of the Tufts chapter of the civil-military relations group, Alliance Linking Leaders in Education and the Services, and the co-director for the 2019 Field Exercise in Peace and Stability Operations. He is also an editor for the Harvard Kennedy School's Singapore Policy Journal.

EXPLORING POLICY CONDITIONS FOR CYBER DETERRENCE: A CASE STUDY OF ESTONIA

There is little disagreement that the proliferation of technology and the internet has dramatically altered conventional concepts of defense. Within the last decade the world has seen a 1052% growth in internet usage,² and countries around the globe continue to pursue further digitization and integration of the Internet of Things (IoT). While this has undeniably brought efficiency and progress, dependence on cyberspace for economic and critical services has only increased. This creates a security conundrum at a time when malicious activity in cyberspace by state and non-state actors seems ever so prevalent. Cyberspace as a fifth dimension of warfare³ is not only relatively new but also relatively unknown. More importantly, it is not yet well understood. Some countries have already begun attempts to secure their own cyberspace and prepare for conflict within it. For example, the United States (US) has designated cyber as an operational domain⁴ and is revamping its Cyber Command to strengthen its ability to conduct defensive and offensive cyber operations.⁵ not all countries are as well-equipped to navigate the perils and uncertainties that are characteristic of cyberspace. There are problems associated with attribution, qualifications of the “use of force”, and proportionality of response with which the international community continues to grapple. Compounding these problems is the difficulty of translating traditional concepts of defense, especially that of deterrence, to cyberspace.

Despite the lack of understanding and consensus on strategies for deterring potential aggressors in cyberspace, analyzing specific responses by small states can provide examples for other, often larger countries. These small states are usually highly centralized and easier to govern, given their comparatively smaller size, allowing them to act as useful policy laboratories. To that end, instructive lessons

² Miniwatts Marketing Group, “World Internet Usage and Population Statistics,” *Internet World Stats*, 2018, accessed July 02, 2018, <https://www.internetworldstats.com/stats.htm>.

³ “War in the Fifth Domain,” *The Economist*, July 1, 2010, accessed July 02, 2018, <https://www.economist.com/node/16478792>.

⁴ David Alexander, “Pentagon to Treat Cyberspace as “Operational Domain,” *Reuters*, July 15, 2011, accessed July 02, 2018, <https://www.reuters.com/article/us-usa-defense-cybersecurity-idUSTRE76D5FA20110714>.

⁵ Lolita Baldor, “US Finalizing Plans to Revamp Cyber Command,” *Business Insider*, July 15, 2017, Accessed July 02, 2018, <https://www.businessinsider.com/ap-us-finalizing-plans-to-revamp-cyber-command-2017-7>.

can be drawn through Estonia's experience. In 2007, Estonia suffered a large-scale cyber-attack as part of a domestic incident related to the relocation of a Soviet war memorial known as the Bronze Soldier. Since then, Estonia has become a poster child for cybersecurity and digital expertise. On an international level, it has moved to increase multilateral cooperation among allied nations, spearheaded the North Atlantic Treaty Organization's (NATO) efforts in the cyber realm, hosted NATO facilities like the Cooperative Cyber Defense Centre of Excellence (CCDCOE) and the Cyber Security Range, coordinated international cyber exercises, and signed multiple Cyber Cooperation Agreements with partner states. On the domestic level, it has moved to strengthen its societal will, psychological resilience, and political credibility in the face of potential attackers.

The way in which Estonia responded to the attack, and the subsequent international and domestic policies implemented by the government, demonstrate how deterrence in cyberspace can and should encompass more than its conventional meaning and methods. This shift is necessary because of the radically different nature of cyberspace vis-à-vis conventional domains. In particular, these policies illustrate the possibility of deterrence through denial, multilateral cooperation and promotion of international norms, and increased societal strength and resilience among a state's citizenry. Its experience in successfully translating deterrence to the cyber sphere, where others have struggled, points to the need for an expansion of contemporary deterrence theory to address the inherent difficulties of cyberspace.

Hence, the overarching argument of this piece is that a broader conception of deterrence is needed to meet the challenges of the cyber domain—one that adopts differentiated approaches that include a range of political, diplomatic, social, educational and technological responses. Such approaches would include bilateral exercises, involvement in international organizations, and government restructuring among others. The first part of this article will look at deterrence in cyberspace more broadly: what deterrence means, the problems cyberspace creates, why an expansion in understanding is needed, and the alternative forms of deterrence available. The second part of the article will be a historical account of the 2007 Cyber-Attacks, and a brief analysis of the Estonian context. Having gone through the types of deterrence available, the third part of the article will look at the policies Estonia has enacted at the international level in line with its

deterrence strategy. The fourth part of the article will similarly look at the domestic level policies implemented by Estonia. The fifth part of the article will then identify and review the challenges facing Estonia's deterrence strategy moving forward.

DETERRENCE AND CYBERSPACE

Cyber-attacks happen every day. In a 2016 report commissioned by the US Government Accountability Office (GAO), a survey of 24 federal agencies found that the number of cyber-attacks climbed 1,300% between 2006 and 2015, from 5,500 to more than 77,000 a year,⁶ with this trend only set to increase. However, against such a backdrop, it is necessary to first understand to what the term cyber-attack refers. There is a myriad of ways an attacker can negatively affect a target system: Denial of Service attacks,⁷ use of ransomware or other destructive malware, stealing information by infiltrating a system, etc. To technically account for all of them would be futile, so for the purposes of a policy discussion such as this one, we will use a RAND Corporation definition for cyber-attacks as the deliberate disruption or corruption of a system of interest by one actor to another actor.⁸ It is important to note here that, as stated in the same RAND report, this definition will exclude cyber espionage and theft, otherwise known as Computer Network Exploitation. This is because a) it does not deprive the user of the full use of the cyber system, b) the user suffers no consequential harm other than having secrets stolen, and c) the laws of war rarely recognize espionage as a *casus belli*. However, the question remains how to deter such cyber-attacks if their scope and methods are so broad and diverse.

Deterrence, as a concept, is not new; it has been around since Thucydides wrote about the Peloponnesian War and framed deterrence as a strategic interaction

⁶ United States Government Accountability Office, "Information Security - Agencies Need to Improve Controls over Selected High-Impact Systems," 2016, 4-5.

⁷ A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it, the services it renders, and the resources it offers inaccessible to its intended users. This can be accomplished by flooding the target with traffic or sending it information that triggers a crash. Definition retrieved from "What is a Denial of Service attack (DoS)?" *Cyberpedia*, accessed April 11, 2019, <https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos>.

⁸ Martin Libicki, "Cyberdeterrence and Cyberwar," USAF Report, *RAND Corporation*, 2009, 23-24.

problem.⁹ It has since been best understood through the modern context of the build-up of nuclear weapons and conventional military means. At the height of the Cold War, it was the deterrent narrative of Mutually Assured Destruction (MAD) that kept the US and the Soviet Union from launching into full-scale thermonuclear war in the face of ideological and geostrategic competition. The principle of massive retaliation against the scepter of any nuclear threat guided the grand strategy of administrations from both countries. It was simply the risks and scale of response that prevented rash action by any one party. The same could be easily applied in conventional military situations, where strong armed forces serve as deterrents to guard against potential geopolitical conflicts. Israel and Singapore are immediate examples that stand out in this regard.¹⁰

However, within these aforementioned analogies lies a major challenge of translating deterrence to cyberspace. Implicit in the logic behind these analogies is the appealing concept of clear, tangible, and proportional retaliation. Also known as deterrence by punishment, this conception of deterrence has arguably been the normative understanding of deterrence theory internationally since the Cold War. However, the very nature of cyberspace makes such a concept of deterrence almost impossible to achieve. Common definitions from the International Organization of Standards and the United Nations (UN) share a similar understanding of the cyber realm: unlike the more familiar domains of the air, land, and sea, the intangible domain of cyberspace is difficult to comprehend and secure owing to its cross-domain scope and complexity.¹¹ Cyberspace is multidimensional, and it involves both public and private entities. The sheer number and diversity of users in cyberspace renders it impossible for governments to have the same degree of control over it as in the physical space.¹² Yet, it is the medium through which many of society's services are provided.

These challenges of cyberspace pose three key issues for deterrence

⁹ Richard N. Lebow, "Thucydides and Deterrence," *Security Studies* 16.2 (2007): 179.

¹⁰ Xing Hui Kok, "Why S'pore needs a deterrent military force," *Today Online*, January 18, 2014, accessed July 03, 2018, <https://www.todayonline.com/singapore/why-spore-needs-deterrent-military-force>.

¹¹ "Resources: Cyber Definitions," *NATO CCDCOE*, 2012, accessed July 03, 2018, <https://ccdcoe.org/cyber-definitions.html>.

¹² Eugene E.G. Tan, "Cyber Deterrence in Singapore," *The RSIS Working Paper Series* 309 (2018): 1-2.

by punishment. Firstly, in cyberspace, actors are no longer able to calibrate the proportionality of their responses. The communal nature of cyberspace means that it provides the foundations for not only social activity but also for economic, military, and malicious activity as well. What we are left with is a domain in which any action might have unforeseen and much further-reaching consequences than initially expected. Deterrence by punishment then quickly becomes troublesome, if not unfeasible. An actor is no longer confidently able to ascertain a proportional response to a cyber-attack that falls within the intended threshold of damage without risking escalation or international condemnation.¹³ Without the ability to gauge outcomes with certainty, the collateral damage caused by a key point of contention could be unintentionally catastrophic.

Secondly, it is increasingly difficult to attribute attacks in cyberspace to specific actors. Certainly, conventional and nuclear attribution to specific actors is also not always a guarantee. However, there are well-established ways of tracing troop movements, weapon shipments, signatures from radioactive material, and the like to state actors. The barriers for non-state actors to attain the capability for similar actions are also significantly low. Yet, as William Lynn wrote, “whereas a missile comes with a return address, a computer virus generally does not.”¹⁴ The sprawling architecture of cyberspace, with its numerous ports, servers, and routers, creates unique issues of identification and attribution of action unparalleled to the physical world.

Thirdly, there is still a lack of consensus on what constitutes ‘use of force’ in cyberspace due to an absence of an objective, internationally-accepted assessment. States are increasingly finding that traditional law of armed conflict (LOAC) principles apply insufficiently to cyber operations, since a kinetic scope of conflict no longer fits this new type of cyber warfare.¹⁵ Informal rules of conduct in cyberspace have recently been introduced by scholars, the most well-received one being the Tallinn Manual on the International Law Applicable to Cyber Warfare. Rule 11 of the manual states that a “cyber operation constitutes a use of force when

¹³ Ibid., 6-7.

¹⁴ William Lynn III, “Defending a New Domain: The Pentagon's Cyberstrategy,” *Foreign Affairs* 89.5 (2010): 99.

¹⁵ Priyanka Dev, “‘Use of Force’ and ‘Armed Attack’ Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response,” *Texas International Law Journal* 50.2 (2015): 381.

its scale and effects are comparable to non-cyber operations rising to the level of a use of force.”¹⁶ There are also some scholars who believe that, should cyber-attacks employ capabilities that cause, or are reasonably likely to cause, physical damage to property, loss of life, or injury of persons in a manner equivalent to kinetic attacks, they will qualify as the “use of force against...territorial integrity” under Article 2(4) of the UN Charter.¹⁷ However, such efforts at translation lack the mechanisms of enforcement which would enhance the legitimacy of and reciprocity for the LOAC. Also, for the cyber-attacks that do not meet the UN's definition of the use of force — damage to property or to human life— it is unclear how states should respond. With no codified international consensus, states thus take a subjective view of what is lawful. The lack of clear parameters for cyber warfare has created a “grey zone” for conflict, wherein actors can conduct cyber-attacks below the threshold of a legitimate threat in which escalation is calculated to be unwarranted. That this calculation is subjective – and that ramifications of such cyber-attacks are uncertain – is disconcerting to many policymakers for whom cyber deterrence is often viewed as a binary strategy to be applied to state actors within a context of geopolitical competition.¹⁸

These challenges complicate modern deterrence in cyberspace. However, this does not mean it is impossible to translate. At its very core, deterrence is nothing more than a rational cost-benefit analysis.¹⁹ This means the dissuasion of an individual from undertaking an action because their perceived costs outweigh the expected benefit. For the application of deterrence theory to cyber, we must first examine a corollary to this framework of understanding: the offense-defense balance model.²⁰

The offense-defense balance model applies a strain of this cost-benefit calculation to warfighting domains to predict the likelihood of a security

¹⁶ Michael Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 47.

¹⁷ Marco Roscini, “Cyber Operations as a Use of Force,” in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan (Cheltenham, U.K.: Edward Elgar Publishing, 2015), 16-17.

¹⁸ Joe Burton, “Cyber Deterrence: A Comprehensive Approach?” *NATO Cooperative Cyber Defence Centre of Excellence*, 2018, 10-11.

¹⁹ Robert Ayson, *Thomas Schelling and the Nuclear Age: Strategy as Social Science (Strategy and History)* (Abingdon: Routledge, 2004), 56, 124-126.

²⁰ Robert Jervis, “Cooperation Under the Security Dilemma,” *World Politics* 30.2 (1978): 187.

dilemma or conflict escalation, and subsequently, a precipitation of war. When the offense (i.e. the attacking aggressor) has the advantage, it is easier to destroy the other's army and take its territory than it is to defend one's own. When the defense has the advantage, it is easier to protect and to hold than it is to move forward, destroy, and take. Depending on whether the domain is offense dominant or defense dominant, these advantages will influence the behavior and actions of actors in light of perceived costs or incentives. In other words, the offense-defense balance is thus understood as the ratio of the cost of the force required by the attacker to take territory to the cost of the forces deployed by the defender.²¹ For conventional warfare, it is often the case that defense is dominant, due to technological advancements in fortification weaponry and the inherent difficulties that geography and terrain pose to offensive forces. Cost also favors the defense: a missile is certainly much cheaper to manufacture than a fighter jet. However, the offense-defense balance is inverted when applied to cyberspace. Offense is dominant, and since the majority of current network systems were designed with openness and not security in mind, the ability to exploit structural vulnerabilities will always be greater than the capacity to defend and fortify them.²² As Ilai Saltzman puts it, "Cyber capabilities tilt the offense-defense balance in favor of the offense, not in the prospects of gaining and maintaining control over territory and material resources as a manifestation of victory, but rather in the actual possibility to paralyze the enemy's military deployment and civilian preparedness and drastically limit its retaliatory potential."²³ The benefits and likelihood of success that come with cyber-attacks, then, far outweigh the cost calculations of such actions.

Moving away from the traditional lens of deterrence, there is a need for a more comprehensive approach to alter the cost-benefit calculation of potential aggressors. The use of the same frameworks as nuclear and conventional deterrence cannot be sufficient, and a new form must be envisioned. As more individuals, businesses, and governments digitalize, cyber vulnerabilities will continue to pervade society. Cyber-attacks on critical institutions, both public and private, can then have immediate and consequential national security implications.

²¹ Charles Glaser and Chaim Kaufmann, "What is the Offense-Defense Balance and Can We Measure It?" *International Security* 22.4 (1998): 53.

²² Lynn, "Defending a New Domain," 99.

²³ Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance," *Contemporary Security Policy* 34.1 (2013): 44.

Deterring against cyber-attacks on such financial, transportation, and other vital infrastructure is, therefore, equally important as deterring cyber-attacks against military and strategic targets. The cross-domain nature of activities in cyberspace means that industries and stakeholders that were previously only tangential to deterrence efforts (if seen as relevant at all) now have to be equally engaged in a coordinated, national, deterrence effort. If the scope for targets is now wider than before, it only stands to reason that so too should deterrence strategies be more comprehensive. As Joseph Nye remarks, deterrence can still be observed in today's cyber age if we broaden the way we use the concept.²⁴ This article draws attention to this broader concept, while also building on Nye's research to complement gaps in his scholarship.

While cyber-attacks can be carried out by both state and non-state actors, this article will focus mainly on state actors, riding on the experience of the 2007 Estonian cyber-attacks allegedly carried out by Russia. This is because the cyber aspect of international relations is quickly becoming a central point of debate and discussion within the international community, and there is an urgent need for the study of both the role cyber plays in international relations and the conditions by which states can protect themselves in cyberspace. Analyzing the Estonian cyber-attacks through the lens of inter-state interaction and calculus can thus help us better understand the logic of deterrence as applied to international behavior, and make the case for an expansion of that deterrence logic. That being said, the policy suggestions explored through the course of this article are by no means limited to deterrence against state actors. The concepts and principles behind deterrence are equally applicable to non-state actors.

TYPES OF DETERRENCE IN CYBERSPACE

In his paper "Deterrence and Dissuasion in Cyberspace," Joseph Nye mentions four different types of deterrence and dissuasion in cyberspace: threat of punishment, denial by defense, entanglement, and normative taboos.²⁵ His ideas are extremely cogent and take into account the various methods by which a cost-benefit calculus of an adversary can be altered. In this regard, his written

²⁴ Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41.3 (2017): 53.

²⁵ *Ibid.*, 54-55.

propositions of deterrence by threat of punishment and denial by defense in cyberspace are precise. However, I believe that more consideration should be given to the arguments of “deterrence by entanglement” and normative taboos.

Nye defines deterrence by entanglement as “the existence of various interdependencies that make a successful attack simultaneously impose serious costs on the attacker as well as the victim.”²⁶ Essentially, this means giving the aggressor something highly valuable to lose in attacking and disrupting the status quo, which contributes to deterrence. Yet, this is difficult to apply to states that are small and have limited resources in comparison to larger countries. While certainly not impossible, the correlation between size and clout is such that a country like Russia would find entanglement, economic or otherwise, less of an issue when engaging in conflict with its smaller neighbors. In this case, I find the capacity for resistance to be a more relevant factor in altering an aggressor’s cost-benefit analysis. Nye’s conception of normative taboos as “detering actions by imposing reputational costs”²⁷ is a valid one but can also afford to be expanded upon. This goes beyond just reputational costs and should also include the creation of frameworks for normative behavior and conflict resolution. Hence, this article will adapt his ideas to create a more encompassing conception of cyber deterrence which would include deterrence by punishment, deterrence by denial, multilateral cooperation and promotion of international norms, and capacity building.

Deterrence by Punishment

As previously discussed, classical deterrence is most often associated with deterrence by punishment. Just as the use of conventional and nuclear weapons helps to inform the decisional calculus of any potential attacker, so too can the use of offensive cyberweapons. Yet, I have previously shown that due to problems of attribution and uncertainty in knowing the exact type of retaliatory damage that will be incurred, such retaliatory threats of punishment are less likely to be effective in cyberspace. However, punishment is still possible through the Diplomacy, Information, Military, Economic, Financial, Intelligence, and Law Enforcement (DIMEFIL) model.²⁸ Responses need not be within the same domain, but rather

²⁶ Ibid., 58-60.

²⁷ Ibid., 60-62.

²⁸ Jelle van Haaster, “Assessing Cyber Power,” in “2016 8th International Conference on Cyber Conflict,” 18, <https://ccdcoe.org/multimedia/8th-international-conference-cyber-conflict->

on a spectrum extending horizontally outside that domain. This affords the state a degree of flexibility in choosing a response that appeals to its strength. These may include economic sanctions, foreign policy maneuvering, releasing of information, etc.

Deterrence by Denial

While deterrence by denial was not often considered a feasible strategic option during the nuclear Cold War era, it is perhaps one of the most promising forms of deterrence in cyberspace. When the adversary is unknown, the timing of the attack is uncertain, and the intents are unclear, increasing the costs of an attack through good defense can discourage an adversary from even attacking. The harder it is for the attacker to achieve his objectives, the less incentive he will have to attack. Such defenses can also prolong the adversary's efforts, making him commit more time and resources without the guarantee of success. These difficulties disrupt the cost-benefit model of the attacker, and discourages further attacks by attempting to tilt the offense-defense balance back in favor of the defense. The side-effect of creating more resilient systems is a greater capacity for the state to recover after an attack, which is valuable in itself.

Multilateral Cooperation and Promotion of International Norms

Creating a conducive and stable environment for the use of cyberspace is only possible through an internationally agreed-upon, rules-based order. This can and should serve as a framework that guides the behavior of both state and non-state actors, resulting in predictability and security through common understanding. The key is to establish international norms through supranational organizations and multilateral cooperation, forming expectations and taboos that could serve to impose reputational costs on actors who fail to comply. This would be sustained by confidence-building measures such as bilateral exchanges and international dialogue as well as cooperation through forensic assistance. Such frameworks must also include dispute resolving mechanisms and avenues for redress and punishment. This will both prevent and reduce the risks of unintended escalation of incidents in cyberspace, and will provide a measure of as-

surance to all actors regarding mutual compliance and normative behavior. Without such an international system, actors' behavior will be less predictable and the stability of the international environment will be jeopardized - the strong will do what they can, and the weak will suffer what they must.

Capacity Building

The importance of robust systems cannot be understated in efforts to discourage potential attacks. If attackers cannot realize their objectives, there will likely be less motivation to attack. However, while similar to deterrence by denial, capacity building puts less emphasis on the technical aspects of cyber defence and more on the peripheral and holistic factors that complement it. These factors include increasing societal strength and resilience, bolstering political processes and will, and raising the level of national readiness through backup systems and disaster drills.

Taken individually, these concepts are necessary but insufficient conditions for establishing a successful deterrence strategy in cyberspace. It is only by drawing on the totality of these concepts that credible signals about a state's capability, resilience, and intentions can be made through coherent policy making. This must be done through a whole-of-government – and even a whole-of-nation approach – requiring close coordination across all relevant government and civil agencies.

SETTING THE CONTEXT: ESTONIA'S SECURITY OUTLOOK AND THE 2007 CYBER-ATTACKS

Estonia provides an informative case study demonstrating how to leverage the various government and civil levers to establish an effective response and lasting deterrence against a cyber-attack. Estonia's relatively small economy, population, and geographical size may make it seem to be an unlikely target of a massive cyber-attack, but the country is no stranger to foreign aggression. Having endured multiple occupations – it was subject to the rule of powers such as Denmark, Sweden, the Russian Empire, Nazi Germany, and the Soviet Union – Estonia's need for robust security policies to ensure its own survival is deeply ingrained within its national psyche. Estonia is also keenly aware that its small size renders it disproportionately vulnerable to regional and global conflicts, having fewer resources and international power to mitigate conflicts and crises. It has to respond dynamically to economic shifts and adapt quickly to regional conflicts and changes in the for-

eign policy of its allies. These concerns have spurred Estonia's political leadership to create robust, far-sighted, and holistic policies that address the country's geo-strategic limitations and shortcomings.

Given its experiences, Estonia can be seen as a policy laboratory for the successful application of deterrence in cyberspace. Thus, it is useful to treat Estonia as an "influential case"²⁹ for the expansion of deterrence theory. An influential case is a case that casts doubt upon a theory, and for that reason warrants close inspection. The analysis of the case may reveal that the theory is validated, perhaps in some slightly altered form, contributing to the reconceptualizing of the theory and general model.³⁰ The Estonia experience still confirms the core hypothesis of deterrence theory: the cost-benefit calculation. However, it reveals a need for an expansion of the general model to accommodate for the translation of deterrence to cyberspace.

This vulnerability to the global environment was manifested on April 30, 2007, when Estonia suffered what was at the time considered to be one of the most crippling cyber-attacks on a state: a massive denial-of-service attack on its networks which affected citizens' access to financial and government services. This cyber-attack occurred amidst the overall climate of tension between ethnic Estonians and the country's Russian minority population, spurred by the Estonian government's decision to move a Soviet memorial called the "Bronze Soldier," commemorating the liberation of Estonia from the Nazis, from Tonismagi Park in central Tallinn to the Tallinn Military Cemetery. To ethnic Estonians, the memorial represented a symbol of Soviet oppression, but for the Russian minority, its relocation represented further marginalization of their ethnic identity by the state. As riots broke out on the streets, this nationalist backlash was complemented by distributed denial-of-service (DDoS) attacks targeting key national infrastructure and servers used for email, the web, domain name resolution, and other services.³¹ Systems stalled under unusually high data traffic, exceeding average-day peak loads by a factor of 10. In addition, the political establishment

²⁹ John Gerring, "Case Selection for Case-Study Analysis: Qualitative and Quantitative Techniques," in *The Oxford Handbook of Political Methodology*, ed. Janet Box-Steffensmeier et al. (Oxford: Oxford, 2008), 2.

³⁰ Ibid., 14-15.

³¹ Healey, Jason, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, (Arlington: Cyber Conflict Studies Association, 2013), 19.

was publicly undermined through the defacement of websites and spamming of email inboxes. These attacks affected government websites like those of the Estonian Parliament, and quickly spread to media outlets, financial industries, and banks like Swedbank. This was a multifaceted cyber-attack campaign consisting of a number of distinct attacks conducted over the course of almost four weeks in multiple phases, comprising of not only synchronized human actions but also botnet-based techniques.

Many of the technical response activities to the cyber-attacks were handled by the Estonian Cyber Emergency Response Team (CERT), but after the attacks there were indications attributing the attack to Russia. The Estonian Minister of Justice also asserted that some of the data packets in the overload of data traffic were traced back to IP addresses originating from Moscow offices in the Kremlin.³² Although concrete and indisputable evidence linking Russia to the attacks was hard to obtain, both Estonian officials and academic scholars soon embraced the immediate assumption that Russian authorities were involved. Regardless, the cyber-attack was understood to be the first of its kind that was directed as a coercive instrument in a political conflict against a state.

Interestingly, this attack did not come as a surprise to Estonian authorities. News had been spreading that commenters were rallying within Russian-language security forums online a few weeks before the attacks in an effort to find help initiating low-intensity DDoS attacks against organizational pillars of Estonian society. Governmental officials also knew that with the extent of its society using government e-services, Estonia offered a tantalizing target. However, they had assumed that the cyber-attacks would likely occur in May and coincide with the completion of Estonia's e-Elections, with the expectation that the attacks would be aimed at exposing the vulnerabilities of their electronic voting systems.³³

A task force had been set up to continuously monitor the Estonian internet during the elections in an effort to reduce such risks, and, after the election proceeded uneventfully, the task force was on standby. Yet, there was an inability to centrally monitor national internet services, and the cyber-attacks were only confirmed through mutual updates between individual technical operators in Es-

³² Ryan R. Gelinas, "Cyberdeterrence and the Problem of Attribution," Master's thesis, Georgetown University, 2010, 8-9.

³³ "Joint Research Project: Interview with Lauri Almann, BHC Laboratories," interview by author, June 01, 2018.

tonia. In fact, there was a serious breakdown in communication, as coordination between key personnel both within the government and with the private sector mainly occurred through sauna sessions and informal interactions instead of clear lines of institutional communication.³⁴ Allegedly, there were moments where approval authorities were unclear and major decisions were made without prior approval, such as the shutting down of the entire national internet network for the rebooting of Swedbank's security systems.³⁵

Now more than a decade later, Estonia is a household name in the cyber domain. The tiny nation-state has built itself a strong international reputation for its expertise in cyber defense and cybersecurity. It has successfully managed to optimize policy at both the systems level and sub-systems level, involving a whole-of-government and whole-of-country approach to create a cyber-operating environment that is safe, monitored, cooperative, and sustained. Its experience of the 2007 Cyber-Attack has offered it an opportunity not only to take a hard look at its own system vulnerabilities, but also to bolster national resilience and exploit other possibilities in the field of cyber. On balance, Estonia has become one of the few countries in the world to recover and bounce back from such a cyber-attack. Looking at how it has done so could provide policymakers with alternative ideas *vis-à-vis* current methods that do not quite seem to work.

As stated in its 2017 National Security Concept, Estonia addresses its own national security as a part of a wider international security. Its small size means that trends connected to globalization and the impact of international crises and conflicts affect Estonia with increasing immediacy. In maintaining its security, Estonia seeks and supports ways and means that have a positive impact on itself as well as on other states. Therein lies the overarching impetus for its specialization in cyber, with two specific, compelling arguments that explain Estonia's push towards an emphasis on cyber.

Firstly, from a strategic point of view, cyber is a domain that is not just constantly growing, but also has the potential to revolutionize a range of sectors. Operations in the military, financial, governance, and resource sectors could be augmented by developments in this field. By leveraging and spearheading these developments, Estonia can not only enhance its own defense and economy, but

³⁴ Ibid.

³⁵ Ibid.

position itself to remain relevant in the global arena and increase its own survival as well. This is especially important since small countries often lack the clout to influence their international environment, and have to strive harder to ensure their survival in a world where you are either at the table or on the menu.

Secondly, the relatively low-cost nature of cyber operations and development makes the industry a sensible option for Estonia to focus on.³⁶ A small economy and lack of manpower means that, in contrast to more intensive primary and secondary industries like manufacturing, and even some tertiary industries like biomedical science, cyber offers a practical and feasible alternative for investment. Indeed, this was one of the key considerations of Estonian officials when choosing cyber as a point of focus for the country. While defensive cyber capabilities could arguably be difficult to stand up, they are at least intensive on the two things that Estonia fortunately has in abundance – technology and human resource.

The process by which Estonia has managed to progress in cyber is worth exploring in order to provide a blueprint for other national efforts in the future to secure this ever-growing paradigm. Its novel use of both international and domestic level policies to achieve a deterrent effect against future attacks casts a shadow on traditional deterrence logic. It also suggests multiple possible levers policymakers have at their disposal.

INTERNATIONAL LEVEL POLICIES

From a foreign policy perspective, Estonia has approached cyber deterrence with a framework that consists of investing in the interests of other powers and signaling its expertise to the international audience. It has sought the buy-in and recognition of many countries towards the importance, potential, and dangers of cyber. More crucially, it has positioned itself as an agenda-setter in the field of cyber by using various multinational organizations and diplomatic agreements to push for its interest and solidify its relevance in the field. It is here that Estonia's endeavors deserve attention for challenging conventional wisdom regarding deterrence in the international realm. Estonia goes beyond contributing to the establishment or enforcement of normative taboos for deterrence; it has committed itself across multiple international platforms to be at the table for the creation of an

³⁶ "Joint Research Project: Matthew Crandall, Tallinn University," interview by author, June 04, 2018.

international environment conducive for its survival, complete with structural levers that reinforce its defensive and deterrent capabilities. This reveals lessons for possible ways deterrence value can be obtained through other foreign policy areas previously thought to be tangential.

The most evident example of this political maneuvering is the NATO CCDCOE. Estonia had initially advocated for the creation of the center in 2003 and, while the details were slowly worked on in the following years, the 2007 Cyber-Attacks helped Estonia to highlight the potential vulnerabilities of other NATO countries and their institutions. Estonia's proposals were well received by other NATO members, and the CCDCOE was set up in Tallinn in 2008. This makes it one out of 12 COEs that "train and educate leaders and specialists from NATO member and partner countries, assist in doctrine development, identify lessons learned, improve interoperability, and capabilities and test and validate concepts through experimentation."³⁷ With a diverse group of experts from 20 nations and mixed military, government, and industry backgrounds, the CCDCOE is one of the few global nexuses for the development of cyber capability and concept of operations.

The CCDCOE is significant both for what it organizes and what it provides which contributes substantially towards Estonia's cyber deterrence. It conducts one of the world's largest and most complex international technical cyber defense exercises, Locked Shields, as well as the annual premier cyber conflict conference, CyCon. It offers a platform for foreign operators to hone their skills, while benefiting NATO and Estonia with the opportunity to enhance interoperability and to learn concepts of operation from other militaries to strengthen cyber resilience.³⁸ It also helps to set parameters on acceptable norms relating to cyber activities and warfare, which goes some way in promoting international behavioral frameworks. Most importantly, it reinforces Estonia's role in the cyber domain, and helps put the country at the forefront by sending a clear signal that Estonia remains a strong player in cyber. The international involvement in the CCDCOE also ensures that enough countries have a stake in Estonia, its

³⁷ "NATO Centres of Excellence," *NATO CCDCOE*, accessed July 14, 2018, <https://ccdcoe.org/nato-centres-excellence.html>.

³⁸ "Joint Research Project: Piret Pernik, International Centre for Defence and Security," interview by author, June 04, 2018.

defense, and its survival. This investment serves as a strong deterrent which gives Estonia both the relevance and the clout it needs to increase its policy space in the international area.

Another example of Estonia's skillful foreign policy is its efforts in the European Union (EU). In 2017, Estonia assumed the rotating presidency of the EU Council of Ministers for 6 months with a clearly articulated intent of making the presidency a digital one.³⁹ Aside from the many other climate, migration, and Brexit-related issues, Estonia put emphasis on positioning itself as the driver for cyber-related issues in the EU by tapping on its niche expertise and the weight of its presidency to highlight the importance of the field in EU affairs. Its achievements in e-governance were a potent source of soft power for Estonia, which it used to push for a digital Europe and work on the free movement of data across all 28-member states.⁴⁰ By the end of its term, it had managed to shift the conversation to technology, build consensus on reform for telecom and chat privacy rules, and rope EU heads of state into a high-level Digital Summit.⁴¹ In addition, Estonia managed to sign e-governance cooperation agreements with the African Union (AU) to develop similar digital systems.⁴² Although conducted with the aim of developing African states and supporting the expansion of trade and service accessibility, it has sparked regional interest in Estonia's cyber offerings and enhanced Estonia's image as a champion for digitalization and cybersecurity.⁴³ Lastly, recognizing that responses to cyber threats require tight coordination across all sectors and all levels of government, Estonia cooperated with the European Defence Agency in 2017 to organize EU CYBRID — a strategic tabletop cyber-exercise for EU Ministers of Defence focused on choices and considerations at the min-

³⁹ Isabelle de Pommereau, "Estonia Takes EU's Helm with Focus on Digitalization, Cyberdefense," *DW*, June 29, 2017, accessed July 14, 2018, <https://www.dw.com/en/estonia-takes-eus-helm-with-focus-on-digitalization-cyberdefense/a-39480254>.

⁴⁰ "Estonia's EU Presidency: Digital Europe and the Free Movement of Data," *e-Estonia*, June, 2017, accessed July 14, 2018, <https://e-estonia.com/estonias-eu-presidency-digital-europe-and-the-free-movement-of-data/>.

⁴¹ "Estonia's Presidency: How it Went," *Politico*, December 20, 2017, accessed July 14, 2018, <https://www.politico.eu/article/estonias-presidency-how-it-went/>.

⁴² Aili Vahtla, "Estonia Signs e-Governance Cooperation Agreement with African Union," *ERR*.ee, December 01, 2017, accessed July 14, 2018, <https://news.err.ee/646044/estonia-signs-e-governance-cooperation-agreement-with-african-union>.

⁴³ "Joint Research Project: Erika Ellamaa, Estonia Ministry of Foreign Affairs," interview by author, June 13, 2018.

isterial level to test crisis responses to a major offensive cyber campaign against EU military structures in a hybrid warfare context.⁴⁴ This helps to harmonize threat perception, situational awareness, and strategic communication processes to ensure common understanding and guide structural responses in the event of any cyber incident. While the explicit emphasis here is on defense, by ameliorating these structural impediments at the inter-government level that would otherwise hinder the effectiveness of any potential reaction, Estonia can be seen as implicitly adding to its deterrent capability through multilateral cooperation. Estonia's ability to respond alongside allied partners in a swift, unified, and decisive manner would decrease the likelihood of a successful attack by aggressors. For a country whose defense strategy relies heavily on the involvement of allied states, this ability is most certainly vital to warning potential adversaries of costly engagement.

Estonia's holistic cyber defense preparations account for not just infrastructure-related vulnerabilities, but also platform-related vulnerabilities pertaining to military equipment. On the bilateral level, Estonia also holds an annual exercise with the Maryland National Guard to simulate response against a cyber-attack on military platforms in the context of a hybrid warfare campaign. The 2017 edition of the exercise, Exercise Baltic Jungle, featured a team of 35 US and 5 Estonian cyber operators at Ämari Air Base pitted against a scenario where a hypothetical adversary had infiltrated malware into computers that run maintenance diagnostics on the US A-10s.⁴⁵ The interwoven use of conventional weapons systems like the A-10 with modern cyberwarfare assets is a model for the kind of complex, multidimensional defensive combat tactics Estonia and NATO need to hone in order to defend themselves from modern hybrid warfare threats. Through exercises like this, Estonia builds on not only its cooperation with allies but also its capability to deny cyber-attacks that occur in parallel to conventional warfare. This serves as an example that there are direct benefits to

⁴⁴ "First Cyber Exercise at EU Ministerial Level Focuses on Strategic Decision-making Tallinn," European Defence Agency, September 7, 2017, accessed July 15, 2018, <https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/09/07/first-cyber-exercise-at-eu-ministerial-level-focuses-on-strategic-decision-making>.

⁴⁵ Nolan Peterson, "A Dress Rehearsal for Defending Estonia From a Putin Invasion," *Newsweek*, September 17, 2017, accessed July 15, 2018, <https://www.newsweek.com/dress-rehearsal-defending-estonia-putin-invasion-666280>.

deterrence in cyberspace deriving from the engagement of tangential elements, such as bilateral exchanges and interoperability exercises.

These international involvements have a tremendous effect on boosting the credibility of Estonia's cyber capabilities. It sends a strong message to potential aggressors that Estonia has the diplomatic clout to table cyber issues at the highest levels of NATO and EU politics, and also that it has the technical expertise to secure its cyberspace and those of its partners. In that same vein, Estonia has also shown its ability to add value in crafting international parameters for acceptable cyber behavior, and to promote interoperability, cooperation, and harmonization amongst friendly partner states. This all serves to enlarge Estonia's security space and signal its investment, as well as that of many international partners, in its security and survival, particularly against cyber operations. It is important to note here how this approach goes beyond traditional efforts of conventional deterrence. Estonia exemplifies an "influential case" in this regard. By using cyber as a diplomatic apparatus, it has managed to create new linkages with allied countries, strengthen defense mechanisms for times of conflict, and crucially, signal its capabilities without directly showcasing them. Such tangential efforts will certainly influence the decisional calculus of state and non-state actors, who are likely to factor in the increased costs arising from Estonia's capacity and international safeguards. From a strategic perspective, Estonia is thus able to burnish its deterrence against any future cyber-attacks. Its experience also reinforces the underlying element of cost-benefit calculation in deterrence, while calling attention to the need for broadening its conceptualization.

DOMESTIC LEVEL POLICIES

On the domestic front, Estonia complements its strategic efforts of deterrence by coordinating policies across the education, social, governance, and defence sectors. This approach creates an environment conducive to deterrence through building societal resilience, establishing national direction, and sustaining military capabilities against cyber threats. As previously argued, the cross-domain nature of cyberspace is such that any attempt at successful deterrence has to engage industries and stakeholders in even seemingly tangential and unrelated sectors. It is no longer sufficient to focus on only the political, economic, and military elements. Thus, working in tandem with one another, policies and directives that seemingly exist in isolation can actually have a cumulative effect on reinforcing

security in cyberspace. Taken together, they present a holistic attempt to increase Estonia's ability to withstand cyber-attacks and decrease the likelihood of success for potential aggressors. This represents a coordinated effort to build capacity for resistance to cyber-attacks and thus increase the costs to aggressors that would lead to successful deterrence. The Estonian experience of successfully increasing deterrence value through acts of nation-building that achieve institutional effectiveness and societal strength serves to reinforce the need to expand the traditional deterrence concept.

In the education sector, Estonia has put an emphasis on policies that build up the talent pool needed to support the state's specialization in the cyber domain. Serving as the foundation for this is a keen understanding that success in this aspect requires attention at not just the higher levels of education, but also at levels as early as first grade. While attracting talent through postgraduate offerings is important, talent-scouting competitions and institutionalized introductory programming courses at the lower tiers are equally necessary for identifying promising individuals and equipping citizens with the necessary computer skills to survive in a digital age. Ultimately, a successful education sector will contribute the cybersecurity manpower and knowledge necessary to strengthen the state and its institutions against the specter of a cyber-attack. This will afford the state not only endurance in the face of a potential attack, but the domestic environment for effective political action as well, adding to Estonia's deterrence capability.

Estonia's universities provide strong academic curricula at the postgraduate level for many cyber-related fields of study. For example, at the Tallinn University of Technology (TTU), the cybersecurity program jointly offered with the University of Tartu since 2010 allows students a unique opportunity to study under professional cybersecurity practitioners hailing from Estonian banks, telecoms, law enforcement, CERT and the NATO CCDCOE.⁴⁶ TTU also offers a master's degree in e-governance technologies and services, focusing on IT solutions at the government level and their impact on the economic, legal, and policy functions of a modern state. These academic programs have all only been introduced within the last decade and are intended to attract and send a clear signal

⁴⁶ "Cyber Security," *Tallinn University of Technology*, accessed August 20, 2018, <https://ttu.ee/cyber-security/#overview-24>.

to prospective students to contribute to Estonia's cyber industry.⁴⁷

Yet, simply creating a talent pool at the university level is insufficient, so Estonia also organizes challenges at the middle to high school stages of education to raise awareness and identify gifted students. In particular, Cybernut and the CyberOlympics are 2 key competitions held annually in-part by the Ministry of Defense.⁴⁸ They are aimed at students, aged 14-19, who are tasked with dealing with malware and encryption, among other cyber tools and problems.⁴⁹ Winners are provided a unique opportunity to visit the most important cyber defence centers in Estonia. It is clear that the intent of these competitions is to foster interest in the cyber domain, as well as to earmark talented individuals for grooming in the cyber field.

At even earlier stages of education still, perhaps the most impressive of its policies is Estonia's ProgeTiger program. In what may be one of the most farsighted education models in the world, ProgeTiger teaches Estonians the foundations of computer programming from as early as kindergarten.⁵⁰ Launched in 2012, this initiative to improve the technological literacy of the entire population from a young age is an investment, made with an eye on equipping future generations with the necessary fluency in information and communications technology disciplines. This program is also in line with developing digital competences through education, one of the eight key competences that the national curriculum focuses on.⁵¹ However, by exposing the young to programming and computer technologies, Estonia is not just ensuring a steady supply of future cyber specialists. It is also making sure that the public will be more familiar with cyber technologies and their associated benefits and detriments, which will be useful for gathering public support and maintaining order in times of crisis and cyber-related incidents. This translates to an increased societal capacity for resilience, as well as greater political

⁴⁷ "Joint Research Project: Anonymous Estonian Ministry of Defense Official," interview by author, June 14, 2018.

⁴⁸ "CyberOlympics 2017/European Cyber Security Challenge 2017 Estonian Preliminary Round," *StudyITin.ee*, May 18, 2017, accessed August 25, 2018, <http://studyitin.ee/en/cyberolympics-2017-european-cyber-security-challenge-2017-estonian-preliminary-round>.

⁴⁹ "First Cyber Defence Competition for Schoolchildren," *StudyITin.ee*, December 31, 2016, accessed August 25, 2018, <http://studyitin.ee/en/estonian>.

⁵⁰ "ProgeTiger Programme," *HITSA*, accessed August 30, 2018, <https://www.hitsa.ee/it-education/educational-programmes/progetiger>.

⁵¹ "FAQ - Digital Competences," *e-Estonia*, accessed August 30, 2018, <https://e-estonia.com/wp-content/uploads/faq-a4-v02-digitalcompetences.pdf>.

maneuvering space for the government to respond to potential cyber threats. Thus, education can create an informed and united domestic front to help decrease the effects of a cyber-attack on the state's population and allow latitude for the government to act. This increases the costs needed for an aggressor to succeed, thereby enhancing the state's deterrence value through denial and capacity building.

In the social realm, Estonia stresses simple cyber hygiene⁵² as the cornerstone for cybersecurity. There is an acute recognition among Estonia's security circles that regardless of the technical defenses and software solutions that can be implemented, it is often a lack of proper individual cyber hygiene training that creates the greatest vulnerability of cyber systems.⁵³ This is taken seriously by the Estonian authorities because of the rate of technological penetration in its society. E-governance is a fixture of daily life and is used to access almost every available government service. Estonians also use state-issued electronic identification cards regularly, which, by design, require two-factor authentication. To this end, Estonia's businesses and government offices frequently go through web-based tests that assess their knowledge of cyber hygiene and seek to mitigate risks associated with such security lapses.⁵⁴ Initiated years ago by the Ministry of Defence, the CybExer cyber hygiene online training was created by the company CybExer Technologies. It was developed to test and improve individual awareness of possible threats in a digital environment, ranging from handling USB drives to opening spam email. Notably, participation in this training has been made compulsory for all civil servants by the Estonian Information System Authority starting 2017.⁵⁵ Putting this kind of emphasis on personal responsibility helps to

⁵² Cyber hygiene refers to activities that computer system administrators and users can undertake to improve their cybersecurity while online. The term cyber hygiene was coined by Vinton Cerf, an Internet pioneer, who used the expression in his statement to the United States Congress Joint Economic Committee in February, 2000.

⁵³ "How Estonia Uses Cyber Hygiene as the Cornerstone of Cyber Security," *Invest in Estonia*, June, 2018, accessed August 30, 2018, <https://investinestonia.com/how-estonia-uses-cyber-hygiene-as-the-cornerstone-of-cyber-security/>.

⁵⁴ "CybExer Technologies Launches a Unique Cyber Hygiene e-Learning Platform," *CybExer Technologies*, May 19, 2016, accessed August 30, 2018, <https://cybexer.com/cybexer-technologies-launches-a-unique-cyber-hygiene-e-learning-platform/>.

⁵⁵ "Estonia Implements CybExer Cyber Hygiene e-Learning Course to All Civil Servants," *CybExer Technologies*, May 18, 2017, accessed August 30, 2018, <https://cybexer.com/online->

ensure the diffusion of cyber defense, right down to the individual level. Taken in the context of society as an entity, this then makes Estonian society less susceptible to cybersecurity oversights and attempts by actors to exploit cyber vulnerabilities. As a result, the chances of a successful cyber-attack drop dramatically vis-à-vis increased costs. This informs the cost-benefit calculus of a potential aggressor, creating a form of deterrence through denial and capacity through collective defense.

On the part of governance, Estonia has committed itself to establishing a clear direction for the state's cybersecurity trajectory. There are two prongs that can be deduced from its efforts post-2008: to institutionalize the strategic conception of cybersecurity development and operations, and to create clearer, more defined decisional and authority chains.

Two crucial documents form the basis of Estonia's domestic cybersecurity policy. The first is the Cybersecurity Strategy, an annually reviewed whole-of-government plan that lays out Estonia's current challenges in cyber and future plans for capability development. Started in 2008, the first iteration of the strategy focused on regulations, organizational setup, and widespread awareness and cooperation across a period from 2008 to 2013.⁵⁶ This marked a stage of transition with regard to conception of cyber from a specialist niche area of expertise to a topic with sprawling implications across significant areas of governance. The Ministry of Defence — in cooperation with the Ministry of Education and Research, the Ministry of Justice, the Ministry of Economic Affairs and Communications, the Ministry of Internal Affairs, and the Ministry of Foreign Affairs — laid down the principles, means of coordination, and regulatory frameworks upon which to build common standards that would transcend both state and private agencies to reduce vulnerabilities at the national level. This included efforts to identify and bolster the security of existing information architecture — such as the X-Road system, a secure national data exchange platform — crucial to the function of the public and private sectors.⁵⁷

Noteworthy is how this iteration of the strategy recognizes that it is “necessary to specify better the distribution of tasks and responsibilities between agencies

training-increases-awareness-of-public-officials-regarding-cyber-hygiene/.

⁵⁶ Cyber Security Strategy Committee, “Cyber Security Strategy,” *Estonia Ministry of Defence*, 2008, 3.

⁵⁷ “Joint Research Project: Anonymous Estonian Ministry of Defense Official,” interview by author, June 14, 2018.

in order to achieve a more efficient organization of cybersecurity of the critical infrastructure and a better coordination of activities in combating cyber threats.”⁵⁸ Following this, in 2009, the Cyber Security Council was added to the government’s Security Committee in order to support inter-agency cooperation and supervise implementation of the objectives of the Cyber Security Strategy. In 2010, the Estonian Informatics Centre was given government agency status and renamed the Estonian Information System Authority, under the Ministry of Economic Affairs and Communications. It received additional powers to maintain the security of the state’s information and communication systems. This also gave them the power to audit private sector security systems to ensure national standards were met.

The second iteration of the strategy moved away from the bureaucratic reformation seen in the first iteration, and instead emphasized technical refinement of cyber capability and national continuity. Recognizing that the advancement of technology was accompanied by “an increase in the state’s growing dependence on already entrenched e-solutions,” there was an expectation of an inevitable rise in the number of potential vectors for, and complexity of, attacks.⁵⁹ This led to an emphasis on protection of critical information systems through a review of alternative solutions for important services, as well as the introduction of virtual embassies that ensure digital persistence “regardless of Estonia’s territorial integrity.”⁶⁰ Aside from fighting cyber-crime, the synchronization of military capabilities for civil cyber emergencies is also stressed to provide for seamless response to defense threats. This is coupled with plans to develop the next generation of cybersecurity professionals, state involvement in cyber research and development (R&D), as well as promoting a legal and international environment conducive for cross-sectoral cyber integration across agencies and global partners. All of this contributes to reinforce the Estonian “cybershield.”⁶¹ At the time of writing, Estonia is still crafting the third iteration of its Cybersecurity Strategy.

⁵⁸ Cyber Security Strategy Committee, “Cyber Security Strategy,” 3,

⁵⁹ “Cyber Security Strategy,” *Estonia Ministry of Economic Affairs and Communication*, 2014, 4.

⁶⁰ Ibid.

⁶¹ “Joint Research Project: Anonymous Estonian Ministry of Defense Official,” interview by author, June 14, 2018.

The other document of significance is the National Security Concept, revised and amended by parliament whenever there are changes in Estonia's security environment. It establishes the objectives, principles, and directions of the state's security policy by taking a broad approach to defense, inter-agency cooperation, and horizon scanning of emerging threats. This sets it apart from the Cybersecurity Strategy, since it takes into account parallel developments in security from a macro perspective. It highlights the role of cyber in terrorism and state conflict, considering its effects not just at the practical and functional level, but also at the societal level. The underlying immutable for the National Security Concept is a strong civil society as the foundation for a strong defense. As it states, "cyberspace may be used for inciting tension and conflicts within the society" and so "attacks against cohesion of Estonian society necessitate greater attention to the sense of cohesion and psychological defense."⁶² This signals a keen understanding of national resilience as a key and intuitive part of defense against cyber-attacks, as seen in the government's efforts in the social and educational sectors, which goes a long way in preparing Estonia for future attacks and lowering the effects they may have on the country.

These policy shifts translate into a definition and prioritization of the national strategic objectives in cyber, maintaining a long-term view of the field that affords it the room to harmonize its advances in cyber with other national strategies and policies. The result is a united cyber front with clarity of direction, organized in alignment with other sectors of government. This reduces the likelihood of success of a cyber-attack, given the tight linkages that afford quick reaction in the defense of critical systems. As such, a reduced calculated chance of success on the part of an adversary will likely deter any potential cyber-attack.

Lastly, on the part of the military, Estonia has swiftly moved to set up cyber capabilities in both the Estonian Defense Forces (EDF) and the Estonian Defense League (EDL). Since 2016, the EDF has been allowing national service conscripts to enlist as cyber experts instead of being streamed into the traditional infantry vocation.⁶³ This leverages enlistee expertise and prevents the wastage of information technology talent, fully utilizing the available resources to buttress the defense of

⁶² "National Security Concept of Estonia," *Riigikogu*, 2010, 8.

⁶³ Raphael Satter, "Cyberconscripts: Baltic Draftees Can Choose IT Over Infantry," *Associated Press*, January 24, 2017, accessed September 02, 2018, <https://apnews.com/3e5b8cc4e63b4630b10fd5186f36ba90>.

the military's electronic equipment. In May 2018, the EDF also launched its Cyber Command into operational status, making official the military's cyber capabilities that are believed to have existed as early as 2005.⁶⁴ The new command will be tasked with carrying out operations to support the ministry and military, while also protecting Estonia's cyber resources, handling everything from training and organization of units to conducting support and information operations.⁶⁵ Interpreted through the lens of defense development, this is part of an effort not just to add value to the present defensive structure of Estonia, but also to explore offensive capabilities that could give the state an upper hand in cyber warfare or retaliation. As Major-General Martin Harem pointed out, "As a small state on the defensive, there is strong cultural and ethical resistance for offensive capabilities. But when dealing with a domain like cyber, if Estonia finds itself having to cross that border, it should have the tools to do so."⁶⁶ This hints at an Estonian understanding of deterrence by denial encompassing more than just static and reactionary cyber defense, but a proactive and forward defense posture that seeks to similarly alter the cost-benefit calculation of a potential aggressor.

The EDL works in tandem with the EDF, functioning as a volunteer, paramilitary organization that serves to enhance the readiness of Estonia's defense. While initially unplanned, the Cyber Defense Unit (CDU) was set up under the EDL in the wake of the 2007 Cyber-Attacks to create professional networks in order to bring together public and private sector expertise.⁶⁷ Its activities include technical training, joint drills with the EDF and international cyber units, educational campaigns, and open-source intelligence analysis. Amongst its ranks are former employees of technology companies like Skype and Microsoft who have both generalist knowledge of the cyber domain and functional specialist competencies that lend themselves to task teams in service of national emergency response agencies. While some of these personnel belong to the military

⁶⁴ "Joint Research Project: Major-General Martin Harem, Estonian Defense Forces," interview by author, June 11, 2018.

⁶⁵ Dario Cavegn, "Defence Forces Cyber Command Takes Up Operations," *err.ee*, August 01, 2018, accessed September 2, 2018, <https://news.err.ee/850719/defence-forces-cyber-command-takes-up-operations>.

⁶⁶ Ibid.

⁶⁷ "Joint Research Project: Lieutenant-Colonel Artur Lillenuurm, Estonian Defense League," interview by author, June 11, 2018.

reserves, some can also be seconded to any ministry if needed.⁶⁸ Indeed, the overarching purpose of the unit is deeply rooted in ensuring the continuous functioning of critical services or deterring threats against such services.⁶⁹ Legal provisions are also made to use the unit in times of crisis to prevent damage to targets deemed to be at high risk of attack. The CDU, then, can also be thought of as serving as a pseudo cyber civil defense force for Estonia.

These military capabilities present a side of Estonia's cyber defense that is perhaps most visible to the international audience. The state has built up these credible institutions to defend its cyberspace, and it is through them that deterrence, both by denial and potentially punishment, can be afforded to politicians as diplomatic apparatus. However, taken in totality with the other domestic policies enacted by Estonia, they only provide one part of an extensive, holistic national approach to cybersecurity. Estonia's domestic planning is comprehensive in not just its conception of cyber and its implications but also the various levers across other government sectors that can be made available in support of cyberdefense. Through this expansive effort, Estonia creates for itself both the reputation and the actual capability to truly be a contending force in the securitization and protection of its cyberspace. While this certainly does influence the perception of costs and benefits involved in a potential attack by an adversary, it is important to take away the extensive and wide-ranging actions Estonia has taken to secure its cyberspace. As an "influential case," Estonia again highlights on the domestic level how an expansion of the conception of deterrence — beyond its underlying conventional principles — is needed for a more complete understanding of the theory.

CONTINUED CHALLENGES

While Estonia has been able to leverage the resources and expertise it has at hand, the act of deterring potential aggressors is a continually holistic and dynamic process. Deterrence is difficult and not always successful; while the defender state is employing its deterrence strategy, aggressor states will always be looking for new ways to overcome it and new metrics for calculating costs. Estonia's continued challenges fit well into this narrative. Despite the suite of policy instruments Esto-

⁶⁸ "Joint Research Project: Anonymous Estonian Ministry of Defense Official," interview by author, June 14, 2018.

⁶⁹ Kadri Kaska, Anna-Maria Osula, and Jan Stinissen, "The Cyber Defence Unit of the Estonian Defence League," *NATO CCDCOE*, 2013, 24.

nia has created for itself, there are still challenges that arise from Estonia's inherent characteristics that come with being a small country. The constraints that a modest economy, comparatively tiny population and workforce, and comparatively fewer resources for R&D present limitations on both Estonia's policy space and competitive viability in the long run. In that vein, while one has immediate policy implications, the other has the potential to adversely affect Estonia's position in the cyber domain. However, taken alongside Estonia's successes, these challenges point to the need for an expansion of deterrence logic as well.

Estonia lacks the ability to leverage its economy in the previously discussed DIMEFIL model of response mechanisms which restricts its options for deterrence by punishment. Despite having a relatively mature economy with a respectably high rate of real GDP growth – 4.9% in 2017⁷⁰ – Estonia's size means its economic clout is comparatively smaller than larger countries. In addition, its economy is highly dependent on trade, with exports of goods and services amounting to 78% of its GDP in 2017.⁷¹ Indeed, by virtue of the small scale of its economy, one ministry official expressed how Estonia's economic future is decidedly reliant on external trade.⁷² This does not afford Estonia the power of enacting sanctions or trade restrictions with other countries as a retaliatory measure in conflict scenarios. This also affects the amount of diplomatic influence (that often accompanies economic heft) that Estonia is able to wield in international institutions like the EU, further hampering any possibility of consolidating support for economic sanctioning. What complicates matters further is the extent of trade relations with Russia, the alleged actor of the 2007 Cyber-Attacks. Russia has consistently been one of the largest trade partners for Estonia in the past few years, being Estonia's fifth largest export destination in 2008.⁷³ This has since only increased, with Russia becoming the third largest export destination and second largest import originator for Estonia in

⁷⁰ "World Factbook: Estonia," *Central Intelligence Agency*, 2017, accessed September 17, 2018, <https://www.cia.gov/library/publications/the-world-factbook/geos/en.html>.

⁷¹ "Estonia: Exports, Percent of GDP," *Global Economy*, 2017, accessed September 17, 2018, <https://www.theglobaleconomy.com/Estonia/Exports/>.

⁷² "Joint Research Project: Karel Lember, Estonia Ministry of Economic Affairs and Communications" interview by author, June 4, 2018.

⁷³ Ibid.

2016.⁷⁴ These interdependencies severely hinder Estonia's ability to credibly utilize economic instruments to exact punishment on would-be aggressors. In fact, Lauri Almann expressed his regret in an interview towards Estonia not being able to pursue a response against Russia via economic sanctions through the EU after the cyber-attacks.⁷⁵ This undoubtedly affects Estonia's deterrence capability to some extent and will need to be accounted for during policy planning at the whole-of-government level.

There are also worries among some in the republic's government that Estonia has created for itself a cyber bubble that may eventually burst.⁷⁶ Estonia has been able to build a niche specialization in cybersecurity mostly due to its proactivity in the securitization of cyberspace, being one of the first few countries to view the domain and its threats seriously. The decision to invest in cyber was due to reasons previously discussed, and that strategy has been successful for Estonia thus far. However, Estonia might find itself having to compete with many other, more resource-rich countries also seeking to shore up their capabilities and expertise in cyber for those very same reasons. Among western powers, the US and other European countries like Germany are already restructuring their industries and militaries to cater to the rise of cyber – in particular, Germany has set up its own dedicated agency for the research of cyber technologies in collaboration with its interior and defense ministries.⁷⁷ The concern is that Estonia's unique prominence in the field will not be sustained for long, and its inherent lack of resources and limited talent pool will make it difficult to contest any larger, emerging party seeking to specialize in the field as well. While this may have an effect on its resulting deterrent credibility, it is far from a lost cause because if anything, Estonia has consistently shown its ability to punch above its weight despite its size.

The challenge for Estonia is thus three-fold: to remain relevant in this

⁷⁴ "Estonia," *Observatory of Economic Complexity*, 2016, accessed September 17, 2018, <https://atlas.media.mit.edu/en/profile/country/est/>.

⁷⁵ "Joint Research Project: Lauri Almann, BHC Laboratories," interview by author, June 1, 2018.

⁷⁶ "Joint Research Project: Major-General Martin Harem, Estonian Defense Forces," interview by author, June 11, 2018.

⁷⁷ Andrea Shalal, "Germany, Seeking Independence from U.S., Pushes Cyber Security Research," *Reuters*, August 29, 2018, accessed September 28, 2018, <https://www.reuters.com/article/us-germany-cyber/germany-seeking-independence-from-u-s-pushes-cyber-security-research-idUSKCN1LE1FX>.

fast-evolving domain, to continually explore new ways to value-add in the field, and to keep innovating new ways to defend and deter cyber-attacks. To this end, while Estonia may face future challenges, it does not take away from the need for an expansion of conceptions towards deterrence. Rather, it serves to reinforce the need to think of deterrence in a more comprehensive and encompassing manner than previously done.

CONCLUSION

With technological advancements and exploitative tools being developed at breakneck speeds, cyber is being viewed increasingly by state and non-state actors as a warfighting domain designed to cater to asymmetric warfare. The 2007 Cyber-Attacks marked the turning point in the use of cyber for hybrid warfare, not just for Estonia, but for the world. Its effects, while short of devastating, were nonetheless significant – despite authorities being able to maintain order and recover essential services, the attacks revealed multiple key vulnerabilities in the state's security architecture. Estonia is not the only country susceptible to such actions, yet over the last decade, it has cleverly managed to innovate around this through carefully crafted policy at the international and domestic levels. Its efforts at multilateral and bilateral forums as well as supranational organizations have centered around coalescing international recognition of the opportunities, threats, and detriments of cyber. These strategies have allowed Estonia to posture itself to shape the direction of developments in the cyber domain and push for its interests while cementing its relevance. At the same time, it is also creating an international environment of normative behavior that is conducive for its survival. Domestically, Estonia has complemented its push abroad through strengthening policies across the education, social, governance, and defense sectors. These policies are aimed at shoring up societal resilience, chains of authority, national long-term planning, and military capabilities vis-à-vis cyber threats. Taken together, these international and domestic policies present a holistic attempt to increase Estonia's ability to withstand cyber-attacks and decrease the likelihood of success for potential aggressors. They send a signal of national resolve and a commitment to national defense through diplomatic, military, and societal means. Far from being singular and isolated policy moves, these tightly coordinated efforts – through punishment, denial, multilateral cooperation, and capacity building

– have a cumulative effect of the state’s deterrence framework. It is precisely these empirics which suggest that a broader conception of deterrence is necessary in studying cyber: by moving beyond traditional, materialist-oriented measurements of deterrence, Estonia is better able to deter aggression in the cyberspace, where threats are amorphous, difficult to attribute, and have implications beyond just the state’s military infrastructure and assets. Estonia thus provides a positive and influential case study for governments worldwide, and a shining example of how countries can secure their cyberspace through seemingly unrelated and unintuitive policy areas, linked by a more holistic conception of deterrence theory.

REFERENCES

- Alexander, David. "Pentagon to Treat Cyberspace as 'Operational Domain.'" *Reuters*. Published July 15, 2018. <https://www.reuters.com/article/us-usa-defense-cybersecurity-idUSTRE76D5FA20110714>.
- Almann, Lauri. Interview by Lionel W.H. Oh with Lauri Almann, BHC Laboratories. *Joint Research Project*. Conducted June 1, 2018.
- Anonymous. Interview by Lionel W.H. Oh with Estonian Ministry of Defense Official. *Joint Research Project*. Conducted June 14, 2018.
- Ayson, Robert. *Thomas Schelling and the Nuclear Age: Strategy as Social Science (Strategy and History)*. Abingdon: Routledge, 2004.
- Baldor, Lolita. "US Finalizing Plans to Revamp Cyber Command." *Business Insider*. Published July 15, 2017. <https://www.businessinsider.com/ap-us-finalizing-plans-to-revamp-cyber-command-2017-7>.
- Burton, Joe. "Cyber Deterrence: A Comprehensive Approach?" *NATO Cooperative Cyber Defence Centre of Excellence*. 2018.
- Cavegn, Dario. "Defence Forces Cyber Command Takes Up Operations." *ERR*. Published August 1, 2018. <https://news.err.ee/850719/defence-forces-cyber-command-takes-up-operations>.
- Crandall, Matthew. Interview by Lionel W.H. Oh with Matthew Crandall, Tallinn University. *Joint Research Project*. Conducted June 4, 2018.
- "CyberOlympics 2017/European Cyber Security Challenge 2017 Estonian Preliminary Round." Published May 18, 2017. *Studyitin.ee*. <http://studyitin.ee/en/cyberolympics-2017-european-cyber-security-challenge-2017-estonian-preliminary-round>.

“Cyber Security.” *TTU*. Published August 20, 2016. <https://ttu.ee/cyber-security/#overview-24>.

“Cyber Security Strategy.” *Ministry of Economic Affairs and Communication, Estonia*. Published 2014.

Cyber Security Strategy Committee. *Cyber Security Strategy*. Tallinn, EE: Ministry of Defence, 2008.

“CybExer Technologies Launches a Unique Cyber Hygiene e-Learning Platform.” *CybExer Technologies*. Published May 19, 2016. <https://cybexer.com/cybexer-technologies-launches-a-unique-cyber-hygiene-e-learning-platform/>.

Dev, Priyanka. “‘Use of Force’ and ‘Armed Attack’ Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response.” *Texas International Law Journal* 50.2 (2015): 381-402.

Ellamaa, Erika. Interview by Lionel W.H. Oh with Erika Ellamaa, Estonia Ministry of Foreign Affairs. *Joint Research Project*. Conducted June 13, 2018.

“Estonia’s EU Presidency: Digital Europe and the Free Movement of Data.” *e-Estonia*. Published June 2017. <https://e-estonia.com/estonias-eu-presidency-digital-europe-and-the-free-movement-of-data/>.

“Estonia: Exports, Percent of GDP.” *Global Economy*. Published 2017. <https://www.theglobaleconomy.com/Estonia/Exports/>.

“Estonia Implements CybExer Cyber Hygiene e-Learning Course to All Civil Servants.” *CybExer Technologies*. Published May 18, 2017. <https://cybexer.com/online-training-increases-awareness-of-public-officials-regarding-cyber-hygiene/>.

- “Estonia’s Presidency: How it Went.” *Politico*. Published December 20, 2017. <https://www.politico.eu/article/estonias-presidency-how-it-went/>.
- “First Cyber Exercise at EU Ministerial Level Focuses on Strategic Decision-Making.” *European Defence Agency*. Published September 7, 2017. <https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/09/07/first-cyber-exercise-at-eu-ministerial-level-focuses-on-strategic-decision-making>.
- “FAQ—Digital Competences.” *e-Estonia*. <https://e-estonia.com/wp-content/uploads/faq-a4-v02-digitalcompetences.pdf>.
- “First Cyber Defence Competition for Schoolchildren.” *Studyitin.ee*. Published December 31, 2016. <http://studyitin.ee/en/estonian>.
- Gelinas, Ryan R. “Cyberdeterrence and the Problem of Attribution.” Master’s Thesis. Washington DC: Georgetown University, 2010.
- Gerring, John. “Case Selection for Case-Study Analysis: Qualitative and Quantitative Techniques.” In *The Oxford Handbook of Political Methodology*, by Henry E. Brady, David Collier, and Janet M. Box-Steffensmeier. Oxford: Oxford University Press, 2008.
- Glaser, Charles and Chaim Kaufmann. “What is the Offense-Defense Balance and Can We Measure it?” *International Security* 22.4 (1998): 44-82.
- Haaster, Jelle van. “Assessing Cyber Power.” In *2016 8th International Conference on Cyber Conflict: Cyber Power*. Edited by N. Pissanidis, H. Roigas, and M. Veenendaal. Tallinn, EE: NATO CCD COE Publications, 2016.
- Harem, Martin. Interview by Lionel WH Oh with Major-General Martin Harem, Estonian Defense Forces. *Joint Research Project*. Conducted June 11, 2018.

Healey, Jason. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Arlington: Cyber Conflict Studies Association, 2013.

Huth, Paul. "Deterrence Failure and Crisis Escalation." *International Studies Quarterly* 31.1 (1988): 29-45.

"How Estonia Uses Cyber Hygiene as the Cornerstone of Cyber Security." *IIE*. Published June 2018. <https://investinestonia.com/how-estonia-uses-cyber-hygiene-as-the-cornerstone-of-cyber-security/>.

"Information Security—Agencies Need to Improve Controls over Selected High-Impact Systems." *United States Government Accountability Office*. Report to Congressional Requesters, Washington DC.

Jervis, Robert. "Cooperation Under the Security Dilemma." *World Politics* 30.2 (1978): 167-214.

Kaska, Kadri, Anna-Maria Osula, and Jan Stinissen. *The Cyber Defence Unit of the Estonian Defence League*. Tallinn, EE: NATO CCD COE, 2013.

Kok, Xing Hui. "Why Singapore Needs a Deterrent Military Force." Published January 18, 2014. <https://www.todayonline.com/singapore/why-spore-needs-deterrent-military-force>.

Lebow, Richard Ned. "Thucydides and Deterrence." *Security Studies* 16.2 (2007): 163-188.

Lember, Karel. Interview by Lionel W.H. Oh with Karel Lember, Estonia Ministry of Economic Affairs and Communications. *Joint Research Project*. Conducted June 4, 2018.

Libicki, Martin. "Cyberdeterrence and Cyberwar." USAF Report, Santa Monica: *RAND Corporation*, 2009.

Lillenum, Artur. Interview by Lionel W.H. Oh with Lieutenant-Colonel Artur Lillenum, Estonian Defense League. *Joint Research Project*. Conducted June 11, 2018.

Lynn III, William. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89.5 (2010): 97-108.

"National Security Concept of Estonia." *Riigikogu*. Tallinn, EE, 2010.

"NATO Centres of Excellence." *NATO CCD COE*. <https://ccdcoe.org/nato-centres-excellence.html>.

Nye Jr., Joseph S. "Deterrence and Dissuasion in Cyberspace." *International Security* 41.3 (2017): 44-71.

"OEC: Estonia." *Observatory of Economic Complexity*. Published 2016. <https://atlas.media.mit.edu/en/profile/country/est/>.

Pernik, Piret. Interview by Lionel W.H. Oh with Piret Pernik, International Centre for Defence and Security. *Joint Research Project*. Conducted June 4, 2018.

Peterson, Nolan. "A Dress Rehearsal For Defending Estonia From A Putin Invasion." Published September 17, 2017. <https://www.newsweek.com/dress-rehearsal-defending-estonia-putin-invasion-666280>.

Pommereau, Isabelle de. "Estonia Takes EU's Helm With Focus on Digitalization, Cyberdefense." *DW News*. Published June 29 2017. <https://www.dw.com/en/estonia-takes-eus-helm-with-focus-on-digitalization-cyberdefense/a-39480254>.

"ProgeTiger Programme." *HITSA*. <https://www.hitsa.ee/it-education/educational-programmes/progetiger>.

“Resources: Cyber Definitions.” *NATO CCD COE*. Published 2012. <https://ccdcoe.org/cyber-definitions.html>.

Roscini, Marco. “Cyber Operations as a Use of Force.” In *Research Handbook on International Law and Cyberspace*, 233-254. Cheltenham, UK: Edward Elgar Publishing, 2015.

Saltzman, Ilai. “Cyber Posturing and the Offense-Defense Balance.” *Contemporary Security Policy* 34.1 (2013): 40-63.

Satter, Raphael. “Cyberconscripts: Baltic Draftees can Choose IT Over Infantry.” *Associated Press*. Published January 24, 2017. <https://apnews.com/3e5b8cc4e63b4630b10fd5186f36ba90>.

Schmitt, Michael. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.

Shalal, Andrea. “Germany, Seeking independence from U.S., Pushes Cyber Security Research.” August 29, 2018. Accessed September 28, 2018. <https://www.reuters.com/article/us-germany-cyber/germany-seeking-independence-from-u-s-pushes-cyber-security-research-idUSKCN1LE1FX>.

Tan, Eugene E.G. “Cyber Deterrence in Singapore.” *The RSIS Working Paper Series* 309 (2018): 1-30.

“War in the Fifth Domain.” *The Economist*. Published July 1, 2010. <https://www.economist.com/node/16478792>.

“World Factbook: Estonia.” Central Intelligence Agency. Published 2017. <https://www.cia.gov/library/publications/the-world-factbook/geos/en.html>.

World Internet Usage and Population Statistics. *Miniwatts Marketing Group*. Published 2018. <https://www.internetworldstats.com/stats.htm>.

Vahtla, Aili. "Estonia Signs e-Governance Cooperation Agreement With African Union." Published December 1, 2017. <https://news.err.ee/646044/estonia-signs-e-governance-cooperation-agreement-with-african-union>.