COI HYBRID INFLUENCE

Hybrid CoE Paper 8

OCTOBER 2021

Cyber deterrence: A case study on Estonia's policies and practice

PIRET PERNIK

Hybrid CoE

Hybrid CoE Paper 8

Cyber deterrence: A case study on Estonia's policies and practice

PIRET PERNIK

Hybrid CoE Papers are finalized pieces of analysis on a topic related to hybrid threats, based on one or several research questions. They may be either conceptual analyses or based on a concrete case study with empirical data.

COI Hybrid Influence looks at how state and non-state actors conduct influence activities targeted at Participating States and institutions, as part of a hybrid campaign, and how hostile state actors use their influence tools in ways that attempt to sow instability, or curtail the sovereignty of other nations and the independence of institutions. The focus is on the behaviours, activities, and tools that a hostile actor can use. The goal is to equip practitioners with the tools they need to respond to and deter hybrid threats. COI HI is led by the UK.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253800 www.hybridcoe.fi

ISBN (web) 978-952-7282-98-4
ISBN (print) 978-952-7282-99-1
ISSN 2670-2053

October 2021

Hybrid CoE is an international hub for practitioners and experts, building Participating States' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats, located in Helsinki, Finland.

Contents

Introduction

In the 21st century, cyber activities have become a prominent means for nation-states to attain national interests and project power globally. In 2007, denial of service attacks against Estonian websites and digital services were considered a wake-up call for NATO about the use of cyberattacks for political reasons, and an impetus for augmenting investments in cybersecurity in Estonia. Shortly after the attacks, the Estonian government endorsed the first national-level cybersecurity strategy focused on the protection of critical information infrastructure. Since then, Estonia has benefitted from making cyber deterrence a cornerstone of its cybersecurity policies.

This Hybrid CoE Paper will address the question of how successful the country has been in implementing cyber deterrence mechanisms. In doing so, this case study elucidates Estonia's cyber deterrence policies between 2008 and 2021, based on an analysis of strategic documents, and evaluates their effectiveness in deterring cyberattacks. The study illustrates that despite the fact that many scholars and practitioners are unconvinced that cyber deterrence is possible, Estonia has effectively prevented serious harm against its networks from global cyber campaigns that severely affected many other countries (such as NotPetya, WannaCry, Solarwinds/Solarigate, Microsoft Exchange Server vulnerabilities, and Kaseya ransomware). To understand Estonia's cyber deterrence policies and practice, a theoretical framework of layered cyber deterrence developed by the US Cyberspace Solarium Commission will be reviewed.[1] The empirical analysis describes how Estonian cyber deterrence policies and mechanisms have worked, giving examples of policy implementation. Based on the Estonian case study, policy recommendations for the EU and NATO will also be made.

1 Brandon Valeriano and Benjamin Jensen, 'Building a National Cyber Strategy: the Process and Implications of the Cyberspace Solarium Commission Report' (CyCon, July 2021).

Cyber deterrence theory

Since the early 2000s, a substantial body of social science literature has explored the complexity of applying nuclear and conventional deterrence theories to a cyber conflict. Deterrence is understood as a coercive strategy that seeks to prevent an actor from taking an unacceptable action.[2] In other words, it means dissuading someone from doing something by making them believe that the costs will exceed their expected benefit.[3] Deterrence succeeds when the target perceives that the costs and risks of an action outweigh the expected gains.[4] The concept of deterrence is commonly viewed as consisting of two sets of activities: denial and punishment.[5] Many of these writings extend the theory and concepts of conventional warfare to cyberspace, primarily focusing on deterrence by punishment (or cost imposition), nation-state actors, and high-end cyber threats.[6] Low-end cyber activities (cybercrime, cyber espionage, privacy violations, and data leaks), which have thus far had the largest impacts on people's lives and organizations, tend to be overlooked in this literature. A further concern is that these theories tend to offer policy prescriptions but they lag behind in developing theoretical and methodological concepts, and conducting empirical research.[7] To date, only a handful of empirical studies about implementing the deterrence theory in cyberspace exist. Some argue that there is little evidence that deterrence policy (and associated cyber organizational and technical capabilities) have succeeded in deterring adversaries, even though some scholars adjudge that cyber deterrence works at the high end.[8] Moreover, some evidence allegedly demonstrates that cyber deterrence based on nation-state cyber capabilities (including offensive cyberspace operations) has decreased cyberspace stability and stoked nation-state power competition.[9]

A key prerequisite for applying deterrence theory is that cyber threats, expected changes in an adversary's behaviour, and a willingness to punish violations must be clearly communicated by governments who aim to deter. Secondly, defenders must provide reassurance that threats of punishment will not be carried out in the event that their demands are met (i.e., the perpetrator reconsiders their intent and refrains from attacking). Thirdly, defenders must have resolve and the perceived capability to carry out the act of punishment.[10] In practice, these prerequisites are commonly missing in nation-state and non-state actors' interactions through cyberspace. This is because cyberspace is inherently different from the nuclear and conventional domains (for example, attribution is difficult, and cyberspace operations are stealthy, to name a few differences). Critics of cyber deterrence

2 Glenn Snyder, *Deterrence and Defense* (Princeton, NJ: Princeton University Press, 1965), cited in: Erica D. Borghard and Shawn W. Lonergan, 'Deterrence by denial in cyberspace', *Journal of Strategic Studies* (2021), DOI: 10.1080/01402390.2021.1944856.
3 Joseph S. Nye Jr., 'Deterrence and Dissuasion in Cyberspace', *International Security*, Volume 41, Issue 3, (2017): 44-71.
4 Robert J. Art, Joseph S. Nye Jr., 'Deterrence and Dissuasion in Cyberspace', *International Security*, Volume 41, Issue 3, (2017): 44-71; Robert J. Art, 'To What Ends Military Power?', *International Security*, Volume 4, Issue 4, (1980): 3-35, cited in: Borghard and Lonergan, 'Deterrence by denial in cyberspace'.
5 Scholarship on cyber deterrence theory includes additional components: entanglement, dissuasion, deflection, inducements, influence, etc. See discussion on these components in Alex Wilner, 'US cyber deterrence: Practice guiding theory', *Journal of Strategic Studies*, Volume 43, Issue 2, (2019), p. 6, DOI: 10.1080/01402390.2018.1563779. Other scholars discuss deterrence by entanglement and deterrence by legitimization as well. See Stefan Soesanto and Max Smeets, 'Cyber deterrence: The Past, Present, and Future', in *NL ARMS Netherlands Annual Review of Military Studies 2020*, ed. Frans Osinga and Tim Sweijs (The Hague, T.M.C. Asser Press, 2021), 385-400, https://doi.org/10.1007/978-94-6265-419-8_20.
[Unless otherwise indicated, all links were last accessed on 15 September 2021.]
6 This scholarship consists of conflicting poles discussed in detail elsewhere. For example, see Wilner, 'US cyber deterrence', 1-36.
7 Wilner, 'US cyber deterrence', 1-36.
8 For example, see Tim Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy*, Volume 33, Issue 1, (2012): 148-170, DOI: 10.1080/13523260.2012.659597; Wilner,'US cyber deterrence', 1-36; Jason Healey, 'Cyber deterrence is Working – So Far,' *Cyber Brief*, 23 July, 2017, https://www.thecipherbrief.com/cyber-deterrence-is-working-so-far.
9 Jason Healey, 'The Cartwright Conjecture. The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities', in *Bytes, Bombs, Spies: The Strategic Dimensions of Offensive Cyberspace Operations*, ed. Herbert Lin and Amy Zegart (Brookings Institution Press, 2019), 173-194.
10 Alex Wilner, 'US cyber deterrence'.

theory further argue that it is particularly difficult to deter attacks below the threshold of armed attack/use of force. For example, how does one deter cybercrime, cyber espionage and data leaks, or cyberspace influence operations? Last but not least, it is hard to prove after the fact that deterrence actually worked.

However, a number of authors argue that employing deterrence tools that are tailored and customized to different actors across the societal, state and international spectrum makes cyber deterrence possible and successful.[11] For example, some practical tools for cyber deterrence by punishment are cyber or kinetic retaliation, legal prosecution, economic sanctions, and diplomatic isolation, while norms are considered tools for deterrence by denial.[12]

In a similar fashion, Erica D. Borghard and Shawn W. Lonergan argue that deterrence by denial is attainable in cyberspace (however, deterrence by punishment is not).[13] According to Borghard and Lonergan, deterrence by punishment includes cross-domain deterrence (for example, a kinetic or nuclear attack, and non-military means such as economic sanctions) and within-domain deterrence (a strategic cyber attack).[14]

Deterrence by denial in cyberspace consists of two mechanisms: denial and defence. Denial includes three sub-concepts: (1) forward defence (an example is an offensive cyberspace operation to disrupt, deny, or degrade an adversary's offensive cyber capabilities and strategy), (2) cross-domain defence, and (3) domestic defence/resilience. Defence also includes forward defence, but here the aim is not to disrupt an adversary's capabilities or strategy as with denial, but rather to gather intelligence through threat-hunting operations in adversary networks.[15] Resilience is conceived as part of deterrence by denial in cyberspace, and is aimed at "increasing the overall ability to defend networks and assets and rapidly recover".[16] Resilience, simply put, means that computer systems under attack continue to function, absorbing the impact of attacks, adapt quickly and continue delivering a satisfactory level of services. The high degree of resilience can convince an adversary that their actions are unlikely to succeed. Strong resilience implies credible deterrence by denial. For example, an adversarial hybrid campaign strategy can be countered by demonstrating that its aims are beyond reach due to the target's hardened networks.[17]

Hence, resilience is a necessary but not sufficient component of deterrence. NATO leaders similarly consider resilience an important component of deterrence, affirming that "national and collective resilience are an essential basis for credible deterrence and defence [...] and vital in our efforts to safeguard our societies, our populations and our shared values".[18]

11 These authors include: Joe Burton, 'Cyber Deterrence: A Comprehensive Approach?', NATO CCDCOE, 2018, https://ccdcoe.org/library/publications/cyber-deterrence-a-comprehensive-approach/; Mariarosaria Taddeo, 'How to Deter in Cyberspace,' Hybrid CoE Strategic Analysis 9, June-July 2018, https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-9-Taddeo.pdf; Heine Sorensen and Dorthe Bach Nyemann, 'Going Beyond Resilience. A revitalized approach to countering hybrid threats', Hybrid CoE Strategic Analysis 13, November 2018, https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-analysis-13-Sorensen-Nyeman.pdf; Vytautas Keršanskas, 'Deterrence: Proposing a more strategic approach to countering hybrid threats', Hybrid CoE Paper 2, March 2020, https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf.
12 Burton, 'Cyber Deterrence'.
13 Borghard and Lonergan, 'Deterrence by denial in cyberspace'.
14 Borghard and Lonergan, 'Deterrence by denial in cyberspace', p. 11.
15 Borghard and Lonergan, 'Deterrence by denial in cyberspace', p. 11.
16 Borghard and Lonergan, 'Deterrence by denial in cyberspace', p. 11.
17 On resilience as an ingredient of deterrence by denial, see Piret Pernik and Tomas Jermalavičius, 'Resilience as Part of NATO's Strategy: Deterrence by Denial and Cyber Defense', in *Forward Resilience: Protecting Society in an Interconnected World*, Working Paper Series, ed. Daniel S. Hamilton (Washington, DC: Center for Transatlantic Relations, 2016), 99-112.
18 'Strengthened Resilience Commitment', NATO, 14 June, 2021, https://www.nato.int/cps/en/natohq/official_texts_185340.htm.

Layered cyber deterrence

US scholars and practitioners have suggested that layered cyber deterrence is a universal model to be applied not only in the States but also in other countries. The model relies on a whole-of-society approach, which coincidentally has been a cornerstone of Estonia's cybersecurity posture since 2007. The goal of layered cyber defence is to change the cost-benefit calculus of the adversary, and reduce the severity and frequency of cyberattacks. It shapes the adversary's behaviour, denies them benefits and imposes costs. A layered cyber deterrence strategy connects means to ends in order "to achieve clear victory conditions in cybersecurity".[19] The components of layered cyber deterrence are presented in Table 1

The first layer of cyber deterrence is an outgrowth of entanglement directed towards shaping the global cyber stability. This activity entails creating cyber norms, international institutions, regulations and law that encourage responsible state action in cyberspace. The second layer advocates denial, domestic defence and resilience, including activities to harden the defences of networks, systems, infrastructures, and assets. The third layer of the deterrence strategy develops tools for imposing costs to coerce adversaries to abide by established norms and rules. It comprises activities that signal to the adversary the consequences of malicious actions.[21]

As malicious cyber activity cannot be stopped with a single action, applying layered deterrence through a whole-of-society approach is expected to prevent cyber risk escalation.[22] The main difference between denial and punishment is that with denial the aim is to defend domestic networks, whereas with punishment the aim is to respond to a malicious cyber action or to communicate a capability and an intent to do so. If cyberspace operations are used for disrupting, denying or degrading an adversary's offensive cyberspace operations and strategy, or for increasing the costs of achieving their objectives, they are considered part of denial (and not punishment).[23]

TABLE 1. Components of layered cyber deterrence.[20]

1st LAYER	**Entanglement and norms:** cyber norms, international law, international organizations, institutions, regimes, regulations
2nd LAYER	**Denial (domestic defence/resilience):** hardening networks, crisis management and rapid recovery after incidents, military cyber defence and intelligence gathering, some offensive cyberspace operations
3rd LAYER	**Punishment:** public attribution, and response measures (economic sanctions, indictments, travel bans, use of military and retaliatory cyberspace operations)

19 Valeriano and Jensen, 'Building a National Cyber Strategy'.
20 Adapted from Valeriano and Jensen, 'Building a National Cyber Strategy', and Borghard & Lonergan, 'Deterrence by denial in cyberspace', p. 11.
21 Valeriano and Jensen, 'Building a National Cyber Strategy'.
22 Valeriano and Jensen, 'Building a National Cyber Strategy'.
23 Borghard and Lonergan, 'Deterrence by denial in cyberspace', p. 11.

The Estonian approach to layered cyber deterrence

Estonia does not have a standalone policy of cyber deterrence, but strategic documents relating to national security, foreign policy and cybersecurity describe diverse components of cyber deterrence. Cybersecurity is deemed a part of foreign, security and defence policy, as well as domestic/internal security. It is also included in strategic documents and policies concerning digital modernization, technology, education and research, and so forth.

The review and analysis of Estonia's strategic documents associated with cybersecurity (presented in Annex I) shows that two concepts – cross-domain deterrence and cyber deterrence – play an important role in the government's cybersecurity discourse. Three layers of deterrence – entanglement and norms, denial and punishment – are equally upheld. Generally speaking, the analysis demonstrates that in the Estonian national security discourse, deterrence by denial and punishment tend to be conceptualized in the context of national security and defence policy; entanglement and norms in the context of foreign policy and cyber diplomacy; and denial (domestic defence/resilience) in the context of digital and technology policies.

As shown in Table 2, cyber deterrence was salient in the cybersecurity strategy that was endorsed by the Estonian government in September 2014. Arguably, the illegal annexation of Crimea by Russia in February 2014 had a profound impact on Estonian national security thinking, including the drafting of cybersecurity strategic documents. It likely sharpened the focus on cyber threats from nation-state and non-state actors related to the national security and constitutional order of the republic.

In contrast, cyber deterrence did not feature in the 2008–2013 document, which was drafted after the 2007 cyberattacks against Estonia's government, bank, media, and other websites, largely because military cyber defence and hybrid threats were omitted from that document due to time and resource constraints.

In the latest strategy (2019–2022), cyber deterrence is referenced almost as frequently as in the 2014–2017 document, apart from the fact that cross-domain deterrence and military deterrence are not mentioned. Rather, concerns about challenges relating to digital modernization and technology policies come to the fore in this strategy. The last column of Table 2 provides examples of how a deterrence tool has been implemented.

It should be noted that different deterrence tools can contribute to several logics/forms of deterrence. For example, a high degree of cybersecurity competence helps to defend domestic networks (deterrence by denial) and simultaneously contributes to Estonia's reputation as a leader in cybersecurity in the international arena, which helps to attain its cyber diplomacy goals (herewith, corresponding to deterrence by entanglement and norms).

TABLE 2. Deterrence tools of national cybersecurity strategies

Deterrence logic/form[24]	Deterrence mechanism/tool	Document	Example
Deterrence by denial; deterrence by punishment	**Military cyber defence**	Strategy 2014–2017	US-Estonia cyber threat-hunting operations
Deterrence by denial; deterrence by punishment	**Collective cyber deterrence through membership of NATO and the EU**	Strategy 2014–2017; Strategy 2019–2022	Active role in the EU and NATO in cybersecurity issues
Deterrence by denial; deterrence by punishment	**Collective cyber deterrence through membership of NATO and the EU**	Strategy 2014–2017; Strategy 2019–2022	Active role in the EU and NATO in cybersecurity issues
Deterrence by denial; deterrence by punishment	**Collective cyber deterrence through membership of NATO and the EU**	Strategy 2014–2017	Signalling that Estonia uses military and non-military responses to cyberattacks
Deterrence by punishment	**Public attribution and response measures**	Strategy 2014–2017; Strategy 2019–2022	Estonia attributed the October 2019 cyberattacks against Georgia to the Russian government
Deterrence by entanglement and norms; deterrence by denial	**International cooperation, international events and facilities**	Strategy 2014–2017; Strategy 2019–2022	Location of CCDCOE and NATO cyber range, Cyber Coalition exercise; CCDCOE exercises and conferences
Deterrence by entanglement and norms; deterrence by denial	**Estonia's reputation as a credible international partner, Estonia's competence in cybersecurity**	Strategy 2014–2017	High positions in ITU and Estonia's cybersecurity indices; leading cyber security initiatives in the EU, NATO, UN

24 Adapted from Borghard and Lonergan, 'Deterrence by denial in cyberspace', p. 11.

Practising cyber deterrence in Estonia

According to Estonian experts, tools for deterrence are cyber norms, international cooperation, information sharing with allies, defence, risk management, law enforcement and public attribution.[25] Estonia's key cyber deterrent measures and tools across the three layers of deterrence strategy are shown in Table 3. Notably, some activities can fall into several layers. For example, international cyber defence exercises simultaneously build domestic defence/resilience (deterrence by denial) but also enable deterrence by entanglement through international cooperation, which increases mutual interdependencies. Signalling military cyberspace capabilities is designated as an activity that contributes to deterrence by denial, but if the capabilities are employed they can be used both for denial and punishment.

Entanglement and norms: a focus on international partnerships

Participating in international cooperation (and in doing so, ensuring Estonia's leading position in international cybersecurity issues) is expected to strengthen deterrence through entanglement and norm-setting. The interdependence and entanglement of cyberspace actors can have deterrent effects.[26] When many countries abide by "the rules of the road" – international law, cyber norms and confidence-building measures – and act responsibly in cyberspace, it creates trust and stability. Countries are interdependent in cyberspace. For example, if one country were to target a public core of the internet (such as terrestrial and undersea cables, internet exchange points, and domain

TABLE 3. Components of Estonia's cyber deterrence posture

1st LAYER	**Entanglement and norms:** cyber diplomacy and norms, active participation and a leading role in international bi- and multilateral cooperation, statements on the applicability of international law in cyberspace, capacity building in third countries, bi- and multilateral cooperation; hosting institutions and international events (exercises, conferences), good international reputation
2nd LAYER	**Denial (domestic defence/resilience):** hardening networks, risk and crisis management, military cyber defence and military cyber organizations, signalling offensive capabilities, awareness-raising
3rd LAYER	**Punishment:** public attribution and response measures

25 Saskia Kiisel, *Eesti küberjulgeoleku tugevdamise võimalused läbi küberheidutuse: Ameerika Ühendriikide Näitel* [Possibilities for strengthening Estonia's cybersecurity through cyber deterrence: the example of the United States] (Tallinn: Estonian Academy of Security Sciences, 2019), https://digiriiul.sisekaitse.ee/handle/123456789/2068.
26 See for example Nye, 'Deterrence and Dissuasion in Cyberspace', p. 58.

name system), such an attack would also impose serious costs on the attacker. In this case, interdependencies in cyberspace are likely to contribute to cyber deterrence because a potential attacker has something valuable to lose. For countries whose economic growth and political regime are highly dependent upon the internet, the prevailing interest is to ensure the stability of cyberspace.[27] International cooperation on cybersecurity increases entanglement. Similarly to entanglement, norms "can deter actions by imposing reputational costs that can damage an actor's soft power beyond the value gained from a given attack".[28] The multilateralization of cyber norms helps to raise the reputational costs of irresponsible state behaviour in cyberspace.[29]

As a small country, Estonia stresses the importance of upholding value- and rule-based international order, including democratic freedoms and human rights in cyberspace, which support Estonian security policy objectives. Small countries in particular benefit from the existence of international rule-based order, and from the extension of the rule of law to cyberspace.[30] Estonia's objective is therefore to establish that international law applies to cyberspace, and states must adhere to global cyber norms. It sees international cooperation and cyber diplomacy as being fundamental to domestic defence and resilience.[31] In the country's view, when states violate norms, they must be held responsible for these actions through collective public attribution and the imposition of response measures. Legal consequences must be imposed upon cyber norm violators.[32] Through international cooperation and cyber diplomacy efforts, states will understand that they are interdependent and that cyberspace stability benefits everyone. Hence, responsible state behaviour is in everyone's interests, which contributes to deterrence by entanglement.

An example of entanglement comprises Estonia's efforts since 2007 to put cybersecurity on the agenda of international and regional organizations (the EU, NATO, UN, OSCE, the Council of Europe, and Baltic and Nordic inter-governmental and parliamentary cooperation formats) on a regular basis. Likewise, Estonia has contributed over many years to the cybersecurity capacity-building of many EU and NATO partners and beyond, believing that this assistance contributes to international stability in cyberspace, and consequently deters malicious cyberattacks. Estonia stresses that sharing cybersecurity information and best practices increases mutual trust and stability in cyberspace, strengthening deterrence and defence.[33] For Estonia, multi- and bilateral international cooperation is a primary means of achieving entanglement and norms-related objectives through whole-of-society and multi-stakeholder approaches. Publishing the government's positions on how international law applies to cyberspace is aimed at influencing other states to adhere to responsible state behaviour in cyberspace.[34]

To strengthen its cyber diplomacy capacity, Estonia established a position in 2018 for an ambassador-at-large for cybersecurity. Estonia is one of the leaders among the Baltic and Nordic countries when it comes to cyber diplomacy. It has been a member of the UN Group of Governmental Experts for many years, and is also a leader in cyber diplomacy education for foreign diplomats.[35] As a member of the UN Security Council in 2020–2021, in June 2021 Estonia organized for the first

27 Nye, 'Deterrence and Dissuasion in Cyberspace', p. 58.
28 Ibid.
29 Ibid.
30 Small states are vulnerable to compromises of international law and this makes them defenders of the international order that protects them. See Adam Lupel and Lauri Mälksoo, 'A Necessary Voice: Small States, International Law, and the UN Security Council', International Peace Institute, April 2019, https://www.ipinst.org/2019/04/a-necessary-voice-small-states-international-law-and-the-un-security-council.
31 On Estonia's efforts in promoting norms, see Matthew Crandall and Collin Allan, 'Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms', *Contemporary Security Policy*, Volume 36, Issue 2, (2015): 346-368, DOI: 10.1080/13523260.2015.1061765.
32 'Estonian contribution on how international law applies to the use of information and communication technologies by states, to be annexed to the report of Group of Governmental Experts on Advancing a responsible state behaviour in cyberspace (2019-21)', the Ministry of Foreign Affairs, https://vm.ee/sites/default/files/estonian_contribution_on_international_law_to_the_gge_may_2021.pdf.
33 'Estonian Foreign Policy Development Plan 2030', the Ministry of Foreign Affairs, https://vm.ee/sites/default/files/Estonia_for_UN/Rasmus/valispoliitika_arengukava_01.07.2020.pdf.
34 'Estonian contribution on how international law applies to the use of information and communication technologies by states', The Ministry of Foreign Affairs.
35 For example, see 'Tallinn Winter School of Cyber Diplomacy', the Ministry of Foreign Affairs, 9-10 February 2021, https://vm.ee/en/tallinn-winter-school-cyber-diplomacy-9-10-february-2021.

time in the Council's history an open meeting on cybersecurity, where it raised the issue of state behaviour in cyberspace in the context of international peace and security.[36] Since 2008, Estonia has hosted the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), which sponsors the publication of world-renowned scholarly works on international law applicable to cyberspace – the Tallinn Manuals 1.0 (2013), 2.0 (2017), and the forthcoming volume 3.0.[37]

Denial: domestic defence/resilience

Deterrence by denial, conceptualized in Estonia primarily as domestic defence/resilience measures, is foundational for the country's cybersecurity posture.[38] Deterrence in this area includes a full spectrum of activities prescribed in the national cybersecurity strategies, in cybersecurity legislation and other relevant ministerial regulations. Some of the resilience-related objectives have remained constant since 2008, such as applying measures to harden networks (for example, standards, risk analysis and management tools, incident response, raising awareness, building cybersecurity capacity and competence, to name a few).[39] In June 2021, Estonia published its first national information security standard entitled E-ITS, which is a guideline for public and private network owners and operators to ensure minimum security standards.[40] The Estonian Information System Authority regularly alerts stakeholders and the general public to cyber threats, vulnerabilities and exploits, and helps them to protect their networks. These activities contribute to deterrence by denial by increasing the ability to protect networks and recover from cyber incidents.

In addition, large-scale international cybersecurity events and international organizations hosted in the country are regarded as elements of deterrence by denial. Estonia has hosted high-level cyber exercises for the EU, for example, and the NATO crisis management exercise – Cyber Coalition – has been held in Estonia. The country is also home to international organizations and networks such as CCDCOE, eu-LISA[41] and EU CyberNet.[42] NATO cyber range and the Estonian Defence Forces cyber range CR14, which is open to partners, are located in Tallinn. Cyber components of the Enhanced Forward Presence troops are thought to contribute to cross-domain deterrence and deterrence by denial. It is considered that international high-level events, and EU and NATO-related organizations and facilities on Estonian soil, signal a strong cyber deterrence posture to potential cyber adversaries.

Government programmes such as data embassies (which hosts government data in foreign governments' secure datacentres abroad) and e-residency (which is an Estonian government programme providing access to digital services for non-residents) are counted as a deterrent by the Estonian cybersecurity community.[43] They are believed to ensure that the government will be able to govern the country (and provide digital services to e-residents and the population) in the event of natural disasters and a foreign military invasion of Estonian territory. The founding of the Estonian Cyber Command in 2018, which develops offensive cyberspace and information operation capabilities, can also be considered an archetype of deterrence – namely "a loud organization", which sends a signal of size and strength of organization to potential adversaries.[44] The Estonian Defence

36 'Presidency in June 2021', the Ministry of Foreign Affairs, June 2021, https://vm.ee/en/activities-objectives/estonia-united-nations/presidency-june-2021.
37 The Tallinn Manuals are scholarly works by distinguished international law scholars that are meant to provide an objective restatement of international law as applied in the cyber context. 'The Tallinn Manual', CCDCOE, https://ccdcoe.org/research/tallinn-manual/.
38 In addition to domestic defence and resilence, as discussed earlier in this article, Borghard and Lonergan include deterrence by denial, forward defence and cross-domain defence, but the latter sub-forms of deterrence are not prominent in Estonia's strategic documents.
39 The 2018 Cybersecurity Act stipulates key obligations to ensure cybersecurity. Cybersecurity Act, Riigi Tetaja [State Courier], passed 9 May, 2018, https://www.riigiteataja.ee/en/eli/523052018003/consolide.
40 'Cybersecurity in Estonia 2021', the Information System Authority, https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisuse_aastaraamat_2021_eng_final.pdf.
41 eu-LISA is the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. See: https://www.eulisa.europa.eu/.
42 EU CyberNet: https://www.eucybernet.eu/vision/.
43 For analysis about cybersecurity risks associated with the Estonian data embassies and e-residency programme, see Piret Pernik, 'E-residency and Data Embassies: A Country Without Borders', *European Cybersecurity Journal*, Volume 2, Issue 1 (2016): 54-61.
44 Jason Healey, 'The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities', 15 July, 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836206.

Forces' cyber conscription and Estonian Defence League's Cyber Defence Unit (established in 2009) similarly augment the military deterrence by denial effect of a loud organization by adding extra human resources, flexibility and agility, as well as by extending their mandate to encompass responding to peacetime incidents and to incidents affecting the private sector.

As discussed, military cyber defence contributes both to denial and punishment measures, depending on the objectives of cyberspace operations. If the goal of a cyberspace operation is threat-hunting across domestic networks, they contribute to deterrence by denial. For example, in 2020 the US Cyber National Mission Force conducted joint cyberspace operations with the Estonian Cyber Command in the Estonian networks to detect and remove malware.[45] As long as such hunting operations do not target an adversary's cyber capabilities and strategy, and do not exceed the Estonian networks, they are considered to be contributing to deterrence by denial and domestic defence/resilience. In contrast, strategic cyberspace operations targeting an adversary's cyber capabilities are deterrence by punishment.

Punishment: public attribution and response

Public attribution can be regarded as a tool for deterrence.[46] Indeed, among Estonian experts, public attribution is regarded as a primary tool of cyber deterrence.[47] As noted by scholars, one aim of public attribution is the act of norm-setting – that is, establishing "the rules of the road" and subsequently enforcing appropriate behaviour in cyberspace (response measures).[48] In a similar manner, the Estonian government holds that "public statements on attribution can be made, with the aim of increasing accountability in cyberspace and emphasising the importance of adhering to international law obligations and norms of responsible state behaviour".[49] The Estonian Ministry of Foreign Affairs subscribes to the opinion that "public attribution [...] allows states to send clear messages and shape expectations that malicious cyberspace operations will not be tolerated" and "it is necessary to send a message that harmful cyberspace operations are not part of acceptable state behaviour".[50] In other words, Estonia directly links public attribution to setting cyber norms, thus connecting deterrence by entanglement and norms to legal consequences, namely deterrence by punishment. According to this view, Estonia supports public attribution and collective measures "where possible" and "public attribution and messaging are tools for deterring and responding [...] but also for raising wider awareness".[51] To support collective public attribution and to hold violators responsible, Estonia actively contributes to EU and NATO cyber deterrence discussions, and belongs to the US-led international cyber deterrence initiative.[52]

The second objective of public attribution (in addition to norm-setting) is coercion – that is, aiming to compel others to stop an activity, or deterring them from doing something by threatening them with unacceptable punishment.[53] This view is also expressed by Estonian government officials and diplomats. For example, Heli Tiirmaa-Klaar, ambassador-at-large for cyber diplomacy, judges that public attribution of cyberattacks itself has

45 'Cybersecurity in Estonia 2021', Information System Authority.
46 For example, see Keršanskas, 'Deterrence'.
47 Kiisel, *Eesti küberjulgeoleku tugevdamise võimalused läbi küberheidutuse*.
48 Florian J. Egloff and Max Smeets, 'Publicly attributing cyber attacks: a framework', *Journal of Strategic Studies*, DOI: 10.1080/01402390.2021.1895117.
49 'Estonian contribution on how international law applies to the use of information and communication technologies by states', The Ministry of Foreign Affairs.
50 'Attribution and Deterrence in Cyberspace', in *Cybersecurity in Estonia 2020*, Information System Authority, https://www.ria.ee/sites/default/files/content-editors/RIA/cyber_security_in_estonia_2020_0.pdf.
51 'Attribution and Deterrence in Cyberspace', Information System Authority.
52 The initiative was announced in the National Cyber Strategy 2018. 'The National Cyber Strategy of the United States of America', the White House, September 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; Eva-Maria Liimets, 'Eestil tuleb vapralt enda eest seista [Estonia must bravely stand up for itself]', ERR, 16 February, 2021, https://www.err.ee/1608111031/eva-maria-liimets-eestil-tuleb-vapralt-enda-eest-seista.
53 While most scholars are critical of the potential to deter or compel adversarial cyber activity, some believe that public attribution can support coercive efforts directly or indirectly. See Egloff and Smeets, 'Publicly attributing cyber attacks'.

a deterrent effect.[54] A similar view is expressed by Urmas Reinsalu, the minister of foreign affairs, who stated that the implementation of the EU's sanctions on Russian entities "sends an ever more important signal at a time when many countries and the medical sector are experiencing increased pressure from cyber attacks".[55] Clearly, as the minister indicated, EU sanctions communicate to Russian hackers that such attacks violate the established rules and norms.

In January 2019, the government adopted public attribution guidelines and established an inter-agency attribution and response options working group.[56] Together with its allies, Estonia regularly engages in public attribution of cyberattacks, and is one of the leading countries in the EU's cyber diplomacy, and in preparing the implementation of the EU's cyber sanctions regime.[57] Recent examples in the framework of the EU's cyber sanctions regime are public attribution of cyberattacks targeting the Organisation for the Prohibition of Chemical Weapons, WannaCry, NotPetya, and Operation Cloud Hopper (in July 2020), as well as cyberattacks against the Bundestag (in October 2020).[58] In March 2020, together with the UK and US governments, Estonia attributed the October 2019 cyberattacks against Georgia to Russia, stating that: "We are clear that Russia's military intelligence service (the GRU) conducted these cyberattacks in an attempt to sow discord and disrupt the lives of ordinary Georgian people. These cyberattacks are part of Russia's long-running campaign of hostile and destabilizing activity against Georgia, and are part of a wider pattern of malign activity. These actions clearly contradict Russia's attempts to claim it is a responsible actor in cyberspace and demonstrate a continuing pattern of reckless GRU cyberspace operations against a number of countries." [59]

In April 2021, the North Atlantic Council (NAC) attributed the SolarWinds/Solarigate cyberattack to Russia,[60] and in July the EU and NATO issued statements attributing cyberattacks against Microsoft Exchange Server to China.[61] The NAC stated that "we acknowledge national statements by Allies, such as Canada, the United Kingdom, and the United States, attributing responsibility for the Microsoft Exchange Server compromise to the People's Republic of China. In line with our recent Brussels Summit Communiqué, we call on all States, including China, to uphold their international commitments and obligations and to act responsibly in the international system, including in cyberspace".[62]

Similarly, at the Brussels Summit in June 2021, NATO leaders denounced Russia's "attempted interference in Allied elections and democratic processes; political and economic pressure and intimidation; widespread disinformation campaigns; malicious cyber activities; and turning a blind eye to cyber criminals operating from its territory, including those who target and disrupt critical infrastructure in NATO countries".[63]

In the past, the Estonian Foreign Intelligence Service has attributed Russian government- affiliated advanced persistent threats to the Russian security services (FSB, SVR and GRU).[64] The so-called hard evidence about the attribution has not been publicly released (it is generally believed that revealing technical details about technical attribution could compromise one's own tactics, techniques, and procedures, harming counter-

54 Välismääraja, 'Heli Tiirmaa-Klaar: küberrünnete omistamine võib aidata neid ennetada' [Attributing cyberattacks can help prevent them], Postimees Podcast, 5 July, 2021, https://kuula.postimees.ee/7286083/heli-tiirmaa-klaar-kuberrunnete-omistamine-voib-aidata-neid-ennetada.
55 'The EU implements its cyber sanctions regime for the first time', The Ministry of Foreign Affairs, 30 July, 2020, https://vm.ee/en/news/eu-implements-its-cyber-sanctions-regime-first-time.
56 'Cybersecurity in Estonia 2020', Information System Authority.
57 'The EU implements its cyber sanctions regime for the first time', The Ministry of Foreign Affairs.
58 'Cyber Diplomacy', The Ministry of Foreign Affairs, June 22, 2021, https://vm.ee/et/tegevused-eesmargid/kuberdiplomaatia.
59 Permanent Mission of Estonia to the UN, 'Stakeout on cyberattack against Georgia by Estonia, the United Kingdom and the United States', 5 March, 2020, https://un.mfa.ee/press-stakeout-by-estonia-the-united-kingdom-and-the-united-states-on-cyberattack-against-georgia/.
60 'North Atlantic Council Statement following the announcement by the United States of actions with regard to Russia', NATO, 15 April, 2021, https://www.nato.int/cps/en/natohq/official_texts_183168.htm.
61 John Hudson and Ellen Nakashima, 'U.S., allies accuse China of hacking Microsoft and condoning other cyberattacks', *The Washington Post*, July 19, 2021, https://www.washingtonpost.com/national-security/microsoft-hack-china-biden-nato/2021/07/19/a90ac7b4-e827-11eb-84a2-d93bc0b50294_story.html.
62 'Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise', NATO, 19 July, 2021, https://www.nato.int/cps/en/natohq/news_185863.htm.
63 'Brussels Summit Communiqué', NATO, 14 June, 2021, https://www.nato.int/cps/en/natohq/news_185000.htm.
64 'International Security and Estonia 2018', Estonian Foreign Intelligence Service, 2018, https://www.valisluureamet.ee/doc/raport/2018-en.pdf.

intelligence capabilities). However, the Estonian authorities annually publish information about Russia's and China's global cyberspace operations and influence campaigns.

In a recent overview of cybersecurity, the Estonian Information System Authority similarly observes that, for the Russian government, "activities directed against other states in cyberspace are merely an instrument to increase its influence and accomplish its objectives". In a number of publications, Estonian authorities warn the general public that Estonian networks and systems are constantly mapped and vulnerabilities are scanned by automated systems "to obtain information that would be useful for planning any kind of large-scale activities against Estonia".[65] The closest thing to attributing a cyberspace operation against the Estonian infrastructure is the Estonian Information System Authority's disclosure that malware and servers used by APT28 (which the Estonian Foreign Intelligence Service attributed to the GRU) were found in the network of a large utility in Estonia.[66]

However, even though in 2020 about 2,700 cyber incidents targeted the confidentiality, integrity and availability of Estonian networks, the Estonian authorities have not publicly attributed cyberattacks which have targeted these networks.[67] All public attributions by the government concern foreign networks. At the same time, serious cyber incidents have recently targeted the Estonian state information systems. For example, the cyberattacks against the Ministry of Justice in July 2020, and attacks in November 2020 against the Ministry of Economic Affairs and Communications, the Ministry of Foreign Affairs, the Ministry of Social Affairs, and other state agencies have not been attributed thus far. The November cyberattack which affected the web servers of several state authorities and leaked the personal data of about 9,000 Estonian residents has not been attributed. An even more serious data leak occurred in July 2021 when a suspected Estonian resident stole the personal data of almost 300,000 Estonian citizens from a state portal (www.eesti.ee) managed by the Estonian Information System Authority.[68] These examples of successful cyberattacks against Estonia illustrate that even though the country holds third place globally in the 2020 International Telecommunication Union (ITU) global cybersecurity index, cyberattacks against Estonia can and do succeed, and the perpetrators have not been held accountable.[69] It should be noted that in the past, few individuals have been convicted of conducting malicious cyber activities aligning with the national interests of the Russian government.[70] Likewise, interviews with Estonian cybersecurity experts illustrate that a majority of experts deem that improving resilience against cyberattacks is a key tool for cyber deterrence. Additionally, the experts preferred diplomatic and political measures (such as public attribution) as a deterrent over imposing costs (such as economic sanctions and other coercive measures). The experts opined that for a small country (with weak relative cyber power) coercive sanctions would make sense only when imposed together with larger countries, and especially in the framework of the EU and NATO.[71] Thus, one reason why Estonia has not unilaterally imposed sanctions (such as travel bans) could be the popular view that this might provoke further attacks against the country or escalate political tensions.

65 '2015 Annual Report of the Estonian Information System Authority's Cybersecurity Branch', Information System Authority, https://www.ria.ee/sites/default/files/content-editors/kuberturve/2015-ria-annual-cyber-report.pdf.
66 '2017 Annual Report of the Estonian Information System Authority's Cybersecurity Branch', Information System Authority, https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria_csa_2017.pdf.
67 One exception to this tradition is the Estonian Internal Security Service, who in the Annual Review of 2021 attributed phishing attacks against Estonian government employees working for the UN to North Korea, and other cyberattacks against Estonian universities to Iranian actors. See 'Annual review 2020-2021', The Estonian Internal Security Service, https://www.kapo.ee/en/content/annual-reviews/.
68 See an overview of cyberattacks in Estonia in 'Cybersecurity in Estonia 2021', The Information System Authority, https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisuse_aastaraamat_2021_eng_final.pdf.
69 'Global Cybersecurity Index 2020', ITU Publication, 2021, https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/.
70 For example, after the 2007 cyberattacks, 20-year-old Dmitriy Galushkevich was fined for defacement of the Reform Party website: Martti Kass, 'Rahutuste ajal Reformierakonna kodulehte rünnanud noormees sai trahvi [Young man who attacked the Reform Party website during the riots given a fine]', *Postimees*, 23 January, 2008, https://www.postimees.ee/1751045/rahutuste-ajal-reformierakonna-kodulehte-runnanud-noormees-sai-trahvi; Ivo Juurvee and Lavly Perling, 'Russia's Espionage in Estonia: A Quantitative Analysis of Convictions', ICDS, 2019, https://icds.ee/en/russias-espionage-in-estonia-a-quantitative-analysis-of-convictions/.
71 Kiisel, *Eesti küberjulgeoleku tugevdamise võimalused läbi küberheidutuse.*

Conclusions and recommendations

In accordance with Estonian cybersecurity policy, deterrence is achieved by combining military and non-military, national and allied deterrence actions and tools in a whole-of-society approach. It is expected that proportional countermeasures will deter the aggressor from attacking. Prevention and credible deterrence are key tenets of the Estonian security and defence policy in all domains (land, maritime, air, and cyber). The concept of cross-domain deterrence has been a fundamental building block of security and defence policy thinking, and has been extended to the area of cybersecurity, where cyber, military and other non-military tools can deter. Deterrence is achieved through the whole-of-society approach advocated since the publication of the first national cybersecurity strategy. A serious cyberattack in the future cannot be ruled out, but Estonia's comprehensive deterrence policy has made it more difficult to execute. However, the possibility of imposing meaningful costs (economic sanctions, indictments, travel bans, etc.) has not been fully developed in the published documents, and not implemented independently of the EU cyber sanctions regime. Even if some deterrence actions seem to work, response measures could be applied more effectively by targeting specific sectors. This means that a wide range of deterrence tools and actions should be applied comprehensively in the whole-of-society approach, together with international partners.

As mentioned earlier, finding empirical evidence confirming that a specific cyberattack was prevented thanks to entanglement and norms, denial or punishment measures is challenging for scholars and practitioners alike. In the last decade, the number of cyber incidents in the Estonian networks has not decreased; on the contrary, in 2020 and 2021, serious cyber intrusions occurred, which were not deterred and have not been publicly attributed. Empirical evidence from other countries shows that despite implementing a deterrence strategy and imposing meaningful costs, the socio-economic impact of cyberattacks has increased globally (for example, between 2019 and 2021 ransomware payouts have increased).[72] The Estonian authorities admit that both nation-state and non-state actors continue to probe the networks – in some cases, successfully. At the same time, after the 2007 cyberattacks, Estonia has not been targeted by strategic cyberspace operations above the threshold of an armed attack, which indicates that deterrence might be working.

Based on the Estonian case study, a policy recommendation for EU and NATO countries is to apply a three-layered deterrence model.[73] First, EU and NATO countries should participate in entanglement and norms measures such as cyber diplomacy and capacity-building globally. Second, they should invest more in denial measures and, third, jointly develop policies for punitive response options, including developing public attribution procedures to enable quick attribution, and systematically implementing sanctions regimes. It would be feasible to establish memoranda of understanding, and operational- and technical-level frameworks to radically improve information- and intelligence-sharing. Participation in cyber defence and crisis management exercises should be open to like-minded NATO partner countries. Joint bilateral cyberspace operations likewise contribute to mutual trust-building and information-sharing, and increase parties' operational and technical competence.[74] Operational- and technical-level joint activities should be regularly practised among allies and with like-minded partners as they contribute to deterrence by denial. Given that NATO's cyber

72 'The State of Ransomware in 2021', Blackfog, 1 September, 2021, https://www.blackfog.com/the-state-of-ransomware-in-2021/.
73 'The United States of America Cyberspace Solarium Commission', Cyberspace Solarium Commission, March 2020, https://www.solarium.gov/.
74 'Cybersecurity in Estonia 2021', the Information System Authority.

response teams are stretched thin due to protecting NATO's own networks, bi- and multilateral collaboration enables countries to share best practices and, in the event of an emergency, to provide mutual rapid assistance in crisis response.

With regard to deterrence by denial, Estonia, together with other EU and NATO countries, should develop a zero trust security strategy and architecture.[75] Zero trust is a cybersecurity paradigm that treats networks as untrusted, and that moves defences from static, network-based perimeters to focus on users, assets, and resources. It assumes that there is no implicit trust granted to user accounts or assets in any network segment (including a corporate local area network), and applies authentication and authorization before a session is established.[76] While deterrence might work at the high end, novel security principles should be implemented by governments because deterrence is not sufficient to deter cyberattacks.

Estonia's public attribution guidelines serve as a blueprint for other countries to attribute cyberattacks and impose meaningful costs. A sharper focus on responses to high- and low-end cyberattacks should be developed in the future along with concrete deterrence actions and tools for individual sectors and target types. For example, deterrence tools can differ for diverse targets: internet voting and e-health systems would be targeted by different cyber threat actors that have political or criminal motives, and the same tool is not effective across all actors.

Estonia's forms of cyber deterrence are not effective individually, nor every time, but when implemented together in a whole-of-society approach, and systematically over a longer period of time, it is likely that many malicious cyberattacks can be deterred. As Joseph Nye pointed out, deterrence tools "can complement one other in affecting actors' perceptions of the costs and benefits of particular actions".[77] Certainly, one cannot deter all cyberattacks – especially those conducted as part of malicious influencing campaigns below the threshold of the use of force – however, it is possible to reduce the number and effect of strategic cyberspace operations. It is likely that punitive responses may deter hostile actors from conducting similar attacks in the future. It will remain to be seen whether the EU and NATO can deter cyberattacks both above and below the threshold of an armed attack better in the future when they apply systematically stronger punitive responses.

75 For example, the US government has released a strategy, architecture and maturity model that the US federal government agencies will implement: 'Moving the U.S. Government Towards Zero Trust Cybersecurity Principles', The White House, https://zerotrust.cyber.gov/.
76 Scott Rose, Oliver Borchert, Stu Mitchell and Sean Connelly, 'Zero Trust Architecture SP 800-207', August 2020, NIST, https://csrc.nist.gov/publications/detail/sp/800-207/final.
77 'Nye, Deterrence and Dissuasion in Cyberspace', p. 62.

Annex I: Cyber deterrence in Estonian, EU and NATO strategic documents

Estonian cyber deterrence policy is based on national, and EU and NATO strategic documents. The following sections describe the role of cyber deterrence in cyberspace in these strategic documents.

National Security Concept 2017

According to the National Security Concept (2017), Estonia's overall deterrence is attained through NATO's collective defence and immediate counteraction and collective countermeasures across military domains, and through Estonia's self-defence measures. Nuclear deterrence is perceived to be an ultimate security warranty for the Alliance. This means that nuclear deterrence extends across all domains, including cyberspace. NATO's cohesion, solidarity, and availability of resources and capabilities is a prerequisite for collective deterrence. In accordance with the concept, deterrence is created through the application of diplomatic, societal, economic, informational and military instruments of national power. In addition to nation-state actors and the military, non-state actors have a role in ensuring credible deterrence in a whole-of-society approach.[78] The section on cybersecurity, however, tends to put stronger emphasis on activities related to defending cyberspace, and does not focus on preventing or deterring cyberattacks before they are launched In addition to cyber defence, a whole-of-society approach and resilience are identified as important for deterrence.

In sum, the concept perceives cyber deterrence as an attribute of broader, cross-domain and collective deterrence, which needs to be implemented through a whole-of-society approach. The ability to wage cyber warfare is viewed as a part of the military defence of the country. The concept addresses the first and second layers in Table 1.

Foreign Policy Development Plan 2030

The Foreign Policy Development Plan 2030 prescribes a number of international activities to ensure a positive cybersecurity image for Estonia globally.[79] The document does not discuss cyber deterrence in detail, but stresses the importance of overall strategic deterrence. As cyber diplomacy falls within the purview of the Ministry of Foreign Affairs, the document revolves around related activities – increasing cyberspace stability, encouraging responsible state behaviour, and deterring irresponsible activities in cyberspace. Participation in the work of international institutions and bilateral cybersecurity cooperation are seen as important tools for increasing cyberspace stability. It is perceived that information- and best practice-sharing, along with trust-building with allies and partners through international cooperation, will increase cyberspace stability, and that Estonia's capability and competence in cyber diplomacy is expected to enable the country to meet global cybersecurity challenges. In sum, this document addresses the first layer of the layered cyber deterrence in Table 1.

78 'The National Security Concept of Estonia', the Ministry of Defence, 2017, https://kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf.
79 'Estonian Foreign Policy Development Plan 2030', the Ministry of Foreign Affairs, https://vm.ee/sites/default/files/Estonia_for_UN/Rasmus/valispoliitika_arengukava_01.07.2020.pdf.

National Cybersecurity Strategy 2008–2013, 2014–2017, 2019–2022

Estonia has published three iterations of the national cybersecurity strategy, covering the periods 2008–2013, 2014–2017, and 2019–2022, respectively.[80] In July 2021, an additional strategic umbrella document was published entitled 'Estonian Digital Society 2030', which provides vision and collaboration principles for the next ten years in the area of cybersecurity.[81]

The scope of the first national strategy omitted the activities of the Estonian Defence Forces in cyberspace, and consequently deterrence as a traditional warfare concept did not appear in the document, which largely focused on the protection of critical information infrastructure, raising awareness of cyber threats, education, legislative and regulative measures, as well as on international cooperation.[82]

The second iteration of the national strategy posited deterrence as one of the three components of military cyber defence, the other two capabilities being early warning and active defence. The document highlighted the relevance of the EU's and NATO's deterrence for the country, and called for active participation in the work of the two organizations with the aim of strengthening collective deterrence in cyberspace. The strategy asserted that a joint cyber threat and situation picture with collaboration mechanisms and procedures among Allies should be created in order to enable strong collective deterrence in the Baltic region.[83] In other words, better monitoring and detection capabilities are expected to improve the Allied cross-domain deterrence. The strategy underscored developing collective countermeasures to respond to cyberattacks as a part of international cooperation.

Credible cyber deterrence was associated with international cybersecurity cooperation and Estonia's efforts to strengthen international cyberspace stability. In this respect, this document communicated a view of the Estonian Foreign Policy Development Plan 2030, but provided more details. For example, hosting international cybersecurity events and cyber exercises in Estonia, establishing NATO-associated facilities (such as NATO's cyber range and NATO CCDCOE located in Tallinn) and other allied infrastructure in the country are considered important for fostering credible deterrence. In like manner, binding agreements with key allies and regular cyber defence exercises and training sessions are seen as mechanisms for implementing cyber deterrence in practice.[84] Notably, Estonia has bilateral cybersecurity and cyber defence agreements with several NATO allies (the US and France), and has established a joint platform for secure cyber threat intelligence-sharing with the US. Thus, operational-level and technical bi- and multilateral cooperation, including information- and intelligence-sharing and technical exercises, are viewed as critical components of strategic deterrence against cyberattacks.[85] This reflects a pragmatic understanding that high-level political declarations and commitment cannot deter cyberattacks, but timely cyber threat intelligence can.

In accordance with the strategy, a necessary element of deterrence is an ability to attribute cyberattacks. The strategy prescribes developing a procedure to attribute attacks, which includes political, legal and technical criteria (this mechanism

80 The fourth and last cybersecurity guideline, which is part of the umbrella document 'Estonian Digital Society 2030', does not mention deterrence and resilience. It focuses on three primary activity areas: domestic cybersecurity governance; analysis of trends, risks, and impacts of cyber threats and cybersecurity; and national capabilities to ensure cybersecurity. The document is published online, but at the time of writing this paper, it has not yet been approved by the government. 'Cybersecurity strategy 2008-2013', the Ministry of Defence (Tallinn, 2018); 'Cybersecurity strategy 2014-2017', the Ministry of Economic Affairs and Communication, 2017, https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf; 'Cybersecurity strategy 2019-2022', the Ministry of Economic Affairs and Communication, 2019, https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

81 The previous iteration of this document entitled 'Digital Agenda 2020 for Estonia' also included guidelines for the development of cybersecurity. The budget forecast for cybersecurity between 2014-2020 was €4.2 million.

82 Piret Pernik and Emmet Tuohy, 'Cyber Space in Estonia: Greater Security, Greater Challenges', Report (ICDS, August 2013), https://icds.ee/wp-content/uploads/2013/Piret%20Pernik%20-%20Cyber%20Space%20in%20Estonia.pdf.

83 'Cybersecurity strategy 2014-2017', the Ministry of Economic Affairs and Communication.

84 Ibid.

85 Estonia engages in informal and formal cooperation and dialogue concerning cybersecurity issues with the Nordic and Baltic countries, the US, the UK, and many other countries. The strategy asserts that substantive cooperation with key partners includes mutual sharing of analyses, technical information and practical knowledge and experiences. The cooperation should consist of political dialogue, regular sharing of analyses, cooperative events and other cooperative formats. See 'Cybersecurity strategy 2014-2017', the Ministry of Economic Affairs and Communication.

was established in 2019) and measures to attribute cyberattacks in the grey zone (below the threshold of armed attack). Estonia must actively attribute attacks together with partners and implement collective countermeasures.[86]

The third iteration of the national cybersecurity strategy (2019–2022) mentions deterrence only four times, indicating a focus on digital policy and economic issues (versus a focus in the previous document on national security and military cyber defence). NATO's collective deterrence against cyberattacks is attained through cyber threat assessment, situational awareness, and attribution and implementing collective countermeasures – hence, it reiterates what was expressed in the earlier version of the strategy. The allied physical presence in the Baltic region is considered a visible demonstration of credible deterrence, signalling NATO's intent and capabilities to domestic and foreign audiences. The strategy again calls for contributing actively to the EU and NATO's cybersecurity, and collaborating with likeminded countries through implementing collective countermeasures, which are expected to improve deterrence. Effective international collaboration with likeminded partners, a good global reputation, and great competency in international cybersecurity matters are considered important for increasing the deterrent effect. In these areas, the document does not add much additional flavour to the understanding of cyber deterrence compared to the previous iteration.

However, it underlines resilience as a part of deterrence. One of the strategy's strategic objectives is to build a sustainable digital society, which will be achieved thanks to strong technological resilience. Another strategic goal, as far as this document is concerned, is to maintain Estonia's position as a leading actor in shaping the international cyber order, duly following the traditional security and defence discourse according to which cooperation with allies and partners enables national cybersecurity to be ensured.

EU and NATO cyber deterrence policies and measures

At the end of 2020, the EU published a renewed cyber security strategy, which states that the identification and prosecution of attackers is necessary to deter cybercrime.[87] The cybersecurity strategy describes a forthcoming cyber deterrence posture that "should outline how the EU and Member States could leverage their political, economic, diplomatic, legal and strategic communication tools against malicious cyber activities, as well as should address how the EU and Member States could advance their ability to attribute malicious cyber activities".[88] The Union has also previously expressed determination to deter cyberattacks through a range of policy instruments and regulations, and has several times used the so-called cyber diplomacy toolbox and legal framework for targeted restrictive measures against cyberattacks, imposing sanctions on individuals and organizations.[89]

Similarly, NATO renewed its cyber defence policy in summer 2021.[90] NATO's measures to counter cyber threats include the full spectrum of tools – military and non-military.[91] Traditional military and non-military instruments of state power can be used to deter cyberattacks, including diplomatic/political, military/intelligence, information, economic, financial, legal and cyber. In addition to the state authorities, a range of non-state actors play an important role in these efforts.

86 'Cybersecurity strategy 2019-2022', the Ministry of Economic Affairs and Communication.
87 'The EU's Cybersecurity Strategy for the Digital Decade', The European Commission, 16 December, 2020, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade.
88 'The EU's Cybersecurity Strategy for the Digital Decade', The European Commission, p. 15.
89 'Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox')', Council of the European Union, 7 June, 2017, https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf; 'Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyberattacks threatening the Union or its Member States', Council of the European Union, 17 May, 2019, https://op.europa.eu/en/publication-detail/-/publication/d4a1c3c8-78ac-11e9-9f05-01aa75ed71a1.
90 NATO endorsed a new Comprehensive Cyber Defence Policy at Brussels Summit 2021, which supports NATO's overall deterrence and defence posture. 'Cyber defence', NATO, 2 July, 2021, https://www.nato.int/cps/en/natohq/topics_78170.htm.
91 Notably, while international relations scholars largely agree that offensive cyber operations will not deter an adversary's conventional military operations on land, and in the maritime, air, and space domains, NATO's position is that the full spectrum of cyber operations (including offensive) can be employed to counter cyberattacks. See 'Brussels Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018', NATO, 11 July, 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

One possibility to deter cyberattacks is public attribution of such attacks by private sector cybersecurity firms, investigative journalists, and NGOs. At the Brussels Summit in 2018, NATO leaders pledged "to employ the full range of capabilities, including cyber, to deter, defend against, and to counter the full spectrum of cyber threats, including those conducted as part of a hybrid campaign".[92] NATO announced that it would develop measures to impose costs on actors who harm the Alliance.[93]

At the latest Summit in Brussels in June 2021, NATO leaders reaffirmed these positions along with the determination to invoke Article 5 of the North Atlantic Treaty to respond to a cyberattack (a decision that would be taken on a case-by-case basis). According to the summit communiqué, NATO considers "possible collective responses to cyberattacks" and will impose costs in response to an attack. NATO also recognized that "the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack". In addition, NATO adopted a renewed comprehensive cyber defence policy, and declared the initial operational capability of its Cyberspace Operations Centre.[94]

92 'Brussels Summit Declaration', NATO.
93 'Brussels Summit Declaration', NATO.
94 'Brussels Summit Communiqué', NATO.

Author

Piret Pernik is a researcher at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). She has researched cybersecurity strategic and policy aspects since 2013. She has published research reports and analyses on cyber resilience, military 5G security, cyber commands, and cyber defence training. She is also a co-editor of the volume *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, published by the CCDCOE. Her articles have been published in academic journals and she has written book chapters, as well as online commentaries. She holds an MA in Social Sciences from the University of Tallinn, and an MA in International Relations and European Studies from the Central European University, Budapest.


Hybrid CoE