# Baltic Cyber Resilience

Baltic Security Foundation

Editors:
OLEVS NIKERS &
OTTO TABUNS

# Baltic Cyber Resilience

Olevs Nikers and Otto Tabuns, editors

Baltic Security Foundation

Riga

2021

# BALTIC SECURITY FOUNDATION

Published by the Baltic Security Foundation
Blaumana iela 9-14
Riga, LV 1011
Latvia
https://www.balticsecurity.eu



This publication was made possible by the support of Microsoft NV.

The printed version of this publication was made possible by the support of Mr. Uldis Šalajevs.

The views expressed in the book are those of the contributors and not necessarily those of any organization or government. For more information on this book of the Baltic Security Foundation, email <info@balticsecurity.eu>.

ISBN 978-9934-23-425-5
Cover art provided by Emīls Garjānis

# Table of Contents

## Introduction

The Baltic states of Estonia, Latvia and Lithuania regained their independence at the beginning of 1990s. Conventional security was at the top of the agenda during that decade while the eviction of Russian army was achieved and the accession to NATO and EU was approved. At the same time, the internet was introduced in the three states, starting with research institutions and expanding into the field of communication, general sourcing of information, commerce and public electronic services.

Cybersecurity rose within a wider societal awareness in all three states in 2007, as the relocation of a Soviet memorial in Tallinn was followed not only by riots but also by cyberattacks sourced to Russia. As noted by the Estonian government, "[a]t the peak of these attacks, fifty-eight Estonian websites were offline at once, including those of the government, most newspapers and banks."[1] This served as a turning point in shaping the perception of what role the information technologies play in the national security of Estonia and the other Baltic states. These events underlined the increased reliance on electronic services and the significance of national capabilities to stay resilient and operational in such a crisis.

Reactions to this included the creation of NATO Cooperative Cyber Defence Centre of Excellence in Tallinn in 2008, the development of

[1] https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/

national policies particular to cybersecurity and national information technology security legislation. In the cases of Latvia and Lithuania, cybersecurity oversight was delegated to the Ministries of Defence. Furthermore, the NATO Energy Security Centre of Excellence, established in Vilnius in 2012 also deals with cybersecurity issues relevant for critical infrastructure, while the NATO Strategic Communications Centre of Excellence, established in Riga in 2014 deals with disinformation that is increasingly projected using cyberspace.

Whereas the development of national cybersecurity policies was inhibited by the aftermath of the global financial crisis of the late 2000's, it did receive additional impetus following the Russian aggression against Ukraine, as NATO decided to recognize cyberspace as another domain of operations in 2016.[2] The European Union laws on the security of network and information systems also progressed in line with the increased awareness of economic and social impact the politically motivated cyber incidents can cause for the largest economic union in the world. So the Baltic states, being members of both organizations, work concurrently with said perspectives when planning and implementing their national policies. Complementary but separate from Baltic involvement in NATO is the bilateral defense cooperation between Tallinn, Riga and Vilnius on the one hand, and Washington D.C. on the other. So it is important to look at these particular links to fully comprehend the Baltic cybersecurity considerations.

[2] Poga, E. "Challenges in Developing Common Cyber Defense", in "Baltic Interoperability Report" (Nikers, O., Tabuns, O., *eds*), 2019, p. 48

The three Baltic states have established a certain cyber resilience and have progressed in national cybersecurity to reach national, regional and international goals. At the same time, many issues remain and many others are emerging, requiring national and collective responses. This report includes the assessment of cybersecurity issues in the three Baltic states, looking at the most important regional, bilateral and multilateral levels outlined above. The contributors have analyzed and prioritized the outstanding issues, proposing specific recommendations for legislation, strategies, policies and practice. The conclusions of the report serve as a guide for national decision makers on assessing the most important gaps and vulnerabilities for national and municipal institutions and their operating procedures.

The report serves to propose and deliver both political and field level gains. On the political level, national institutions can use the conclusions of the report to add to the arguments for specific policy decisions and respective assignment of resources. On the field level, experts at national and municipal institutions have a useful source of reference to develop and implement best practices needed for establishing and developing their information and communication technology systems and electronic government tools.

# Baltics and NATO in cyberspace

*William Watson*

## Introduction

On March 29, 2004, the Baltic States of Estonia, Latvia, and Lithuania joined the North Atlantic Treaty Organization (NATO), providing them with collective security through Article 5 of the alliance. Recently, aggressors have used cyberspace to destabilize the Baltics, collect intelligence, and possibly conduct hybrid warfare, however, these attacks have not met the threshold for use of force. Therefore, the question arises: is an Article 5 response an effective way of deterring and addressing attacks? In addressing the effectiveness of Article 5 in cyberspace, one should analyze the challenges and limitations of Article 5 in cyberspace, how Baltic Countries are threatened in Cyberspace, and finally formulate approaches to Article 5 that address challenges in cyberspace to benefit Baltic security.

## Article 5 of NATO

In 2014, NATO agreed that a cyber attack could trigger Article 5, extending collective security to cyberspace.[3] There are four parts of the article that may be relevant in cyberspace. First, as the article could not have been written in 1949 considering cyberattacks, the idea of a nation conducting a low-scale cyber attack could not be

[3] Porter, Christopher B., July 2019, "*Collective Defense of Human Dignity: The Vision for NATO's Future in Cyberspace*", Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2019/07/Collective_Defense_of_Human_Dignity.pdf

considered.[4] Furthermore, the Article does not instruct how a nation should respond if attacked. As attacks in the cyber realm are frequently dismissed, there is no binding need in the status quo to treat soft attacks against an ally with severity, as you would not treat them with severity if you had been the one attacked.

Second, the Article does not promise direct retaliation against an aggressor, only assistance deemed necessary. The action does have to be aimed at restoring the security of the alliance, meaning that assistance that falls short of restorative action, such as financial aid instead of military retaliation, may not satisfy the article.

Third, the Article does not address what "armed" means in the context of "armed force" and "armed attack."[5] It is unclear if cyber attacks fall under this definition, especially as many attacks do not do substantial damage. The *Tallinn Manual 2.0* suggests that the question of force should be resolved by evaluating the damage done, rather than the weapons used.[6] This question is especially relevant as Baltic countries frequently face the challenge of attacks and disinformation which fall below the threshold for use of force.

Fourth, the Article limits covert action as it requires notification of the UN Security Council. This would prove problematic if a permanent member of the Security Council conducted the attack as

[4] While the definition of low-scale attack may vary, this essay addresses attacks that do not cause loss of life or significant property

[5] Mowery, Samuel P. "Defining Cyber and Focusing the Military's Role in Cyberspace". United States Army War College, https://www.hsdl.org/?view&did=815941

[6] Schmitt, Michael N. "The Use of Force." Chapter. In Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd ed., 328–56. Cambridge: Cambridge University Press, 2017. doi:10.1017/9781316822524.020.

a NATO action could be subject to veto. This has spawned two schools of thought: a French and an American. The French perspective is that the UN has the role of authorizing NATO's use of force. However, given that Russia and China both have permanent seats on the security council, they could veto retaliation against them. The U.S. perspective is that NATO has the right to use force whenever needed by the members.

The current writing of Article 5 limits retaliation and leaves ambiguity in responses. While rewriting the Article may solve some of these issues, the flexibility in response could be a valuable tool to the Baltic region as it may provide retaliation without repercussions, as well as aid without aggression.

**Baltic Security**

The Baltic States face many threats in cyberspace, including cybercrime, cyber espionage, and disinformation. There are worries of hybrid warfare from Russia, similar to what has been seen in Ukraine. President Putin's moves to consolidate ethnic and cultural Russians abroad worries Baltic countries such as Estonia, who see their cities as possible battlegrounds.[7] As Baltic states do not wish to be targets of these attacks, they have increased their defensive capabilities. Historically, Estonia has been the strongest actor in cyberspace, while Latvia and Lithuania have lagged behind. However, cooperation has increased, leading to Latvia and

[7] Josh Rubin, 1-24-2019, "NATO Fears That This Town Will Be the Epicenter of Conflict With Russia," Atlantic, https://www.theatlantic.com/international/archive/2019/01/narva-scenario-nato-conflict-russia-estonia/581089/

Lithuania improving their security.[8] The Baltic states have also partnered with the U.S. to defend its recently independent energy sector from Russian hackers,[9] and increasingly with the EU to decouple their energy from Russia.[10] As of 2020, all three countries have outlined cybersecurity strategies. While defensive measures have increased and NATO has practiced cooperative defense,[11] these measures, as well as each nations' cyber strategy, lack outlines for retaliation, instead focusing on defensive measures.

Estonia has been a target of Russian aggression in cyberspace. In 2007 Estonia was hit by a Russian cyber attack, destabilizing some government services.[12] This attack jumpstarted Estonia's cyber defense and led to the NATO Cooperative Cyber Defense Centre of Excellence's creation and placement in Tallinn. Estonia shows a drive to maintain independence from Russia,[13] likely resulting in their strength in cyberspace. Estonia has launched successful awareness campaigns that educate citizens on proper cyber security, preventing widescale damage from attacks such as NotPetya and WannaCry.[14]

---

[8] Poga, Edgars. March 2019. "Challenges in Developing Common Cyber Defense"(48-49), Baltic Interoperability Report. The Jamestown Foundation.

[9] Mike Parr, 7-10-2019, "US to help secure Baltic energy grid against cyber-attacks," euractiv, https://www.euractiv.com/section/energy/news/us-to-help-secure-baltic-energy-grid-against-cyber-attacks/

[10] Marek Grzegorczyk, 10-2-2020, "Baltic States big winners in allocation of new EU energy infrastructure funding," Emerging Europe, https://emerging-europe.com/news/baltic-states-big-winners-in-allocation-of-new-eu-energy-infrastructure-funding/

[11] E-Estonia Briefing Centre, June 2017, "How Estonia became a global heavyweight in cyber security," e-Estonia, https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/

[12] Kohler, Kevin. "Estonia's National Cybersecurity & Cyberdefense Posture." (2020). https://www.research-collection.ethz.ch/handle/20.500.11850/438276

[13] Grant, Glen. March 2019. "Interoperability Challenges for Meeting Hybrid Warfare Ground Force Threats"(13), Baltic Interoperability Report. The Jamestown Foundation.

[14] Kohler, Kevin. "Estonia's National Cybersecurity & Cyberdefense Posture." (2020). https://www.research-collection.ethz.ch/handle/20.500.11850/438276

Lithuania has been bolstering its cyber security and cooperation. In 2015, after a series of Russian cyber attacks, Lithuania created its National Cyber Security Center.[15] Lithuania led a mutual assistance rapid response cyber agreement amongst EU countries (including Estonia).[16] However, Lithuania faces a different set of challenges that may be better addressed through conventional counter intelligence as Lithuanian travelers to Russia are frequently "pitched" by Russian intelligence to gain information.[17]

Latvia has seen cyber attacks by Russia that fall below the Tallinn Manual's threshold, as Russia intended to conduct espionage, spread disinformation, and cause disruptions.[18] Publicly, Latvia has not pursued strong retaliation against these attacks and their political body has been labeled as "indifferent" toward military affairs.[19]

## Article 5 Applicability to these threats

Article 5 relies on the idea of deterrence to be successful, where aggressors do not attack due to fear of ramifications. In cyberspace,

---

[15] Dalia Bankauskaitė and Vytautas Keršanskas, 2019, "Societal Security and Resilience: Defeating Disinformation Threats", Baltic Security Strategy Report, Jamestown Foundation. https://jamestown.org/wp-content/uploads/2019/09/Baltic-Security-Strategy-Report-2019.pdf?x98343

[16] Anna Varfolomeeva, 6-25-2018, "Six EU states sign declaration on 'rapid response' cyber force," Defense Post, https://www.thedefensepost.com/2018/06/25/lithuania-cyber-rapid-response-pesco/

[17] Olevs Nikers, 3-30-2020, "Baltic Intelligence Agencies Increasingly Worry About Threats From China in Addition to Russia," Jamestown, https://jamestown.org/program/baltic-intelligence-agencies-increasingly-worry-about-threats-from-china-in-addition-to-russia/

[18] Krista Viksnins, 6-23-2020, "Cyberwarfare in Latvia: A Call for New Cyberwarfare Terminology," Foreign Policy Research Institute, https://www.fpri.org/article/2020/06/cyberwarfare-in-latvia-a-call-for-new-cyberwarfare-terminology/

[19] Grant, "Interoperability Challenges for Meeting Hybrid Warfare Ground Force Threats"(14)

there are two types of deterrence: defensive and offensive. Defensive deterrence relies on preventing an attack from having serious ramifications. As most cyber attacks are single use due to actors fixing vulnerabilities, an ineffective cyber attack is unlikely to be launched. Further methods such as using “sandboxes” and “honeypots” can isolate malware, allowing defenders to study attacks.[20] While defense may help safeguard systems, attacks are frequently more sophisticated than their defensive counterparts.[21]

Offensive deterrence refers to retaliation against an attack that is severe enough to discourage aggressors. Cyber counter striking has significant risks. Tit-for-tat retaliation allows adversaries to gain an understanding of their vulnerabilities, without a decisive conclusion.[22] Cyber attacks are also dangerous as they may spill beyond their intended target.[23] Finally, cyber retaliation may exacerbate the conflict by raising tensions to a dangerous level.[24] However, Article 5 is not limited to cyber retaliation and scholars have considered other methods of retaliation to respond.[25]

Article 5 allows for any action deemed necessary to restore security. While not a trade organization, NATO members could conduct

---

[20] Kesan, Jay P. ; Hayes, Carol M., "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace," Harvard Journal of Law & Technology 25, no. 2 (Spring 2012): 429-544

[21] Binnendijk, Anika, and Miranda Priebe. An Attack Against Them All Drivers of Decisions to Contribute to NATO Collective Defense. RAND Corporation Santa Monica United States, 2019.

[22] Kallberg, Jan & Burk, Rosemary A. (2017) “The Flaw of Immediate Cyber Counter Strikes, Strategic Analysis”, 41:5, 510-514, DOI: 10.1080/09700161.2017.1343265

[23] Kosseff, Jeff, Collective Countermeasures in Cyberspace, 10 NOTRE DAME J. INT’L & COMP. LAW.

[24] Касенова, М. Б. "Кибербезопасность и управление интернетом. Документы и материалы для российских регуляторов и экспертов." (2014).

[25] Limnéll, Jarno, and Charly Salonius-Pasternak. Challenge for NATO: Cyber Article 5. 2016.https://www.diva-portal.org/smash/get/diva2:1119569/FULLTEXT01.pdf

proportionate responses through diplomatic, legal, or trade channels.[26] Diplomatic expulsions have been a tool to retaliate against foreign espionage.[27] Legally, NATO countries should continue participation in projects such as the Tallinn Manuals and offer legal assistance to pursue retribution for a cyber attack. Ideally, legal suits would be enough to deter cyber attack; however, the lack of consensus and enforcement mechanisms make this route difficult.[28] Trade sanctions have been used against states in response to cyber attacks. While the Baltic States have been economically distancing themselves from adversarial countries including Russia,[29] there may still be avenues for them, or the Alliance collectively, to conduct proportional responses through sanctions. For example, if a cyber attack did $10 million in damages, there may be a way to levy $10 million in sanctions across the alliance. Giving aggressors the option of paying for the damages done by a cyber attack or suffering sanctions provides clear accountability for cyber attacks. Assistance should be provided when NATO members are affected by the costs of sanctions or counter sanctions. As the Baltic states have been heavily dependent on Russia for exports and energy,[30] assistance would give them more flexibility to levy sanctions against

[26] The Economist, 3-9-2015, "The Economist explains," https://www.economist.com/the-economist-explains/2015/03/09/how-natos-article-5-works

[27] Ahmad, Nehaluddin. "The Obligation of Diplomats to Respect the Laws and Regulations of the Hosting State: A Critical Overview of the International Practices." Laws 9, no. 3 (2020): 18.

[28] Crootof, Rebecca, International Cybertorts: Expanding State Accountability in Cyberspace (March 1, 2016). 103 CORNELL L. REV. 565 (2018), Available at SSRN: https://ssrn.com/abstract=2930700

[29] Bergmane, Una. “Fading Russian Influence in the Baltic States.” Orbis vol. 64,3 (2020): 479-488. doi:10.1016/j.orbis.2020.05.009

[30] Emily Ferris, 7-1-2020, "Unplugging the Baltic States: Why Russia’s Economic Approach May Be Shifting," Russia Matters, https://russiamatters.org/analysis/unplugging-baltic-states-why-russias-economic-approach-may-be-shifting#:~:text=For%20Lithuania%2C%20Russia%20is%20also,fallen%20between%202013%20and%202019.&text=By%202019%2C%20trade%20fell%20by,25th%20top%20trade%20partner.

adversaries. While controversial, increasing trade with aggressors during peace and then reducing trade if an attack occurs gives clear motivators to not attack. Diplomatic, legal, and trade retorsion gives NATO countries options below the use of force. Acting collectively strengthens the alliance and sends clear signals that Baltic countries are subject to NATO protection. Absent clear protections, Baltic countries may see aggression similar to that of Ukraine.[31]

Accountability in cyberspace may be crucial to reduce attacks, however, there is a lack of consensus on the legality of cyber retaliation.[32] While states and academics attempt to come to agreement, the Baltics need mechanisms to strike back against attacks.

## Conclusion

While it is probable that the Baltic countries may benefit from continued NATO defensive support, new approaches must be considered to deter aggression in cyberspace. Article 5 may provide an avenue to retaliate through methods that fall below the use of force, including diplomatic expulsion, sanctions, and legal assistance. Baltic states should push to flex the muscle of NATO to serve as a reminder of the alliance's commitment, protecting themselves and the Alliance. While retaliation in cyberspace has multiple legal and pragmatic implications, collective diplomatic retaliation may increase the safety of the Baltics.

---

[31] Josh Rubin, 1-24-2019, "NATO Fears That This Town Will Be the Epicenter of Conflict With Russia," Atlantic, https://www.theatlantic.com/international/archive/2019/01/narva-scenario-nato-conflict-russia-estonia/581089/

[32] Crootof, “Expanding State Accountability in Cyberspace”

# U.S. Cyber Policy and Implications for the Baltics

*Matthew Thomas*

## Introduction

In September 2018, the White House adopted a new cybersecurity strategy. Among the key components of that National Cyber Strategy was the new provision that the United States would now authorize the use of offensive cyber weapons within its deterrence arsenal.[33] Previously, the United States relied, at least officially, strictly on defensive capabilities to deter malign actors. This shift in policy largely followed recent trends in NATO; in 2017, NATO Secretary General Jens Stoltenberg announced that NATO would incorporate cyber weapons[34] into its military operations to deter against cyber threats from malign actors such as Russia, China, and Iran. At the Brussels Summit in 2018, the allies agreed to the creation of a new Cyberspace Operations Center[35] and reaffirmed the use of national cyber capabilities to aid with military operations and deterrence. In many respects, the United States' National Cyber Strategy formalizes in U.S. policy the changes taking place within the broader context of NATO and the return of great power competition.

## Hybrid Warfare

[33] https://www.gmfus.org/publications/offense-new-defense-new-life-natos-cyber-policy
[34] Ibid.
[35] https://www.nato.int/cps/en/natohq/topics_78170.htm

A critical component of that competition as it stands today is hybrid warfare, wherein most cyber operations fall. Hybrid warfare may be defined as the use of many different subversive, mostly nonmilitary, instruments tailored towards specific weaknesses for the purpose of either a) defeating an adversary slowly over time without fighting, or b) influencing policy outcomes in a target country. These tactics typically include obscuring origination and intent, as well as the continuous fluctuation of conflict intensity. In other words, an actor will target specific weaknesses in an adversary, cover his tracks, and increase or decrease the number and severity of attacks over time. In the context of Russian hybrid warfare strategies, cyber attacks are used for a number of purposes. After 2016, the hacking of information systems[36] for the purpose of manipulating election outcomes has received the most attention. But, this is not the only tool in Russia's cyber arsenal, nor the only vulnerability for Western countries. From protecting critical energy infrastructure to safeguarding critical communications links, the breadth of different cyber vulnerabilities deserves NATO's and the United States' focused attention.

## U.S. Cyber Policy

Prior to 2018, U.S. cyber policy fit within an entirely different framework. The cyber domain was long seen as an entirely exceptional field of operations[37], and cyber tools were reserved for that domain. Likewise, cyber capabilities were only shared with a

[36] https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf
[37] https://www.cfr.org/blog/sharing-caring-united-states-new-cyber-commitment-nato

very select few allies. The notion that the United States would be sharing its tightly guarded cyber assets with NATO allies was a departure from Washington's previous modus operandi. Further, the potential use of cyber assets alongside conventional military capabilities with equal weight given to both offensive and defensive instruments was a complete change in the United States' deterrence posture. Previously the twain did not meet, and cyber deterrence was at least officially purely defensive in nature. The change also brings all of NATO closer[38] to the "Five Eyes" partnership of the United States, Canada, the United Kingdom, Australia, and New Zealand, a tight knit signals intelligence (SIGINT) partnership, as SIGINT and cyber capabilities have been traditionally closely related.

For both the U.S. and NATO, changes in cyber policy largely reflect the maturation of that operational domain. As threats grow more complex and interconnected, it no longer makes sense to stovepipe cyber assets and operations to address only cyber threats. Ultimately, the United States' new posture on the use of offensive cyber tools derives from the idea of power projection[39], a deterrence mechanism frequently used in the more conventional sense in the maritime, air, and land domains. Essentially, the premise behind the tactic is to demonstrate the ability to respond effectively to a crisis or attack, thereby convincing the adversary than an attack is not worth the cost it will have to bear. By opening the door to offensive cyber

[38] https://www.cfr.org/blog/sharing-caring-united-states-new-cyber-commitment-nato
[39]https://www.fifthdomain.com/dod/2017/09/14/cyber-is-being-normalized-with-traditional-operations/

operations, and to the use of cyber assets alongside conventional capabilities, the United States has given its military commanders more tools at their disposal to counter all varieties of threats across multiple operational domains and increase the cost of an attack on itself or its allies.

The White House 2018 National Cyber Strategy outlines four key pillars of cyber policy[40]:

- First, “[Protecting] the American People, the Homeland, and the American Way of Life,”
- Second, “[Promoting] American Prosperity,”
- Third, “[Preserving] Peace through Strength,”
- and finally, “[Advancing] American Influence.”

Each of these pillars contains a number of policy goals, such as securing critical infrastructure and federal information networks (under pillar one). For the purpose of this paper, fitting in the context of NATO, the third and fourth pillars are most important.

Under the third pillar, the primary goals are the enhancement of stability in the cyber domain through encouraging adherence to cyber norms and the attribution and deterrence of unacceptable activities in cyberspace. With respect to norms, this will be a tough row to hoe, as malign actors seldom adhere to norms, and will distort the language of treaties and related agreements in order to

[40] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

justify offensive activities in a form of lawfare.[41] The establishment of norms in cyberspace, where attributing and punishing criminal activity is much more difficult than in other domains, will therefore be difficult to achieve and even more difficult to enforce. However, by improving capabilities in attribution and deterrence, no easy task either, the United States will make the former goal somewhat more achievable. In order to improve capabilities in attribution and deterrence, the strategy outlines four major action items: leading with objective and collaborative intelligence, imposing consequences for malign activities, building a cyber-deterrence initiative with “like-minded” countries, and exposing and countering malign influence and disinformation campaigns online. For each action item, collaboration with allies, information sharing (within the bounds of reasonable operational security), the ability to create real costs for adversarial activities in cyberspace, and the neutralization of adversaries’ operational success undergird the United States’ strategy.

Under the fourth pillar, one key goal is important in the context of cooperation with NATO: “[Building] International Cyber Capacity.” The main idea behind this objective is to develop strategic partnerships with like-minded countries. By developing these partnerships, the United States can help improve the capabilities of allies that have lagged behind in cyber readiness and build mutual trust in information sharing to counter shared threats. Further, it can

[41]https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=5892&context=faculty_scholarship

increase interoperability to ensure greater shared capacity to conduct cyber operations jointly in times of crisis.

To a great extent, in the NATO context, one more policy item is relevant: preventing allies from developing their 5G infrastructures[42] with Chinese companies and encouraging the use of American 5G technologies instead. A primary reason for this policy is the connection between Chinese technology firms, such as Huawei and ZTE, to the Chinese government. With the implementation of 5G systems, cyber defense will be an even more difficult challenge, and thus, NATO members should be aware that opening up to Chinese technologies in 5G will make them more vulnerable to increased espionage, malign influence, and cyberattacks. As a result of U.S. pressure, 25 NATO allies have committed[43] to excluding Chinese firms from their 5G infrastructures.

**NATO Cyber Policy**

Since 2014, NATO's cybersecurity policy has seen many crucial changes to reflect the increasing sophistication of state-driven cyberattacks.[44] At the 2014 Wales Summit, the allies committed to expanding the Article 5 provision ("an attack on one is an attack on all") to include cyberattacks[45] with effects comparable to a conventional attack. Since then, NATO's primary focus[46] has been

[42] https://www.nato.int/docu/review/articles/2020/09/30/nato-and-the-5g-challenge/index.html
[43] https://www.state.gov/the-transatlantic-alliance-goes-clean/
[44] https://www.gmfus.org/publications/offense-new-defense-new-life-natos-cyber-policy
[45]https://ccdcoe.org/incyder-articles/nato-summit-updates-cyber-defence-policy/#footnote_1_2663
[46] https://www.gmfus.org/publications/offense-new-defense-new-life-natos-cyber-policy

its own institutional infrastructure and networks, while encouraging and supporting various programs to help member states bolster their own cyber defense capabilities. Many countries have adopted cybersecurity strategies[47] that adopt whole-of-government approaches, encourage public-private partnerships, and commit to participation within NATO and EU cooperative frameworks on cybersecurity. Likewise, since 2016, NATO and the EU have been cooperating[48] on information sharing, training, exercises, and research on key cyber defense issues. At the 2016 Warsaw Summit, NATO members signed the Cyber Defense Pledge[49], binding them to prioritize upgrades to their cyber defense capabilities. In 2017, NATO announced that it would incorporate assets traditionally reserved for the cyber domain into its military operations (see introduction).

This brings us to the 2018 Brussels Summit. This summit reaffirmed[50] both the 2014 expansion of Article 5 to include particularly damaging cyberattacks as well as the 2017 incorporation of cyber tools within military operations. It was at this time as well that the allies agreed to set up the aforementioned Cyberspace Operations Center in NATO's strengthened command structure. Finally, in February 2019, NATO members endorsed an updated toolkit[51] for responding to malicious cyber activities.

---

[47] https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE329/RAND_PE329.pdf
[48]https://www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=The%20policy%20establishes%20that%20cyber,intensifies%20NATO's%20cooperation%20with%20industry.
[49] https://www.nato.int/cps/su/natohq/official_texts_133177.htm
[50] https://www.gmfus.org/publications/offense-new-defense-new-life-natos-cyber-policy
[51]https://www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=The%20policy%20establishes%20that%20cyber,intensifies%20NATO's%20cooperation%20with%20industry.

NATO policy and U.S. policy in the cyber domain follow largely the same premises and serve the same ends. Both have adopted the position that cyber assets may be used alongside conventional military capabilities. Both seek to more firmly establish the rule of law, norms, and values in cyberspace and punish malign activities. Both prioritize cooperative approaches with allies, promoting information sharing as well as sharing capabilities. Both policies respond to growing adversarial competition, particularly with rising powers Russia and China, and the increased sophistication of these actors' malign cyber operations. Within NATO, however, member states have varying levels of cyber preparedness[52], and individual countries' policies and strategies vary.

## Implications for the Baltics

As small states with limited resources on NATO's eastern flank, Lithuania, Latvia, and Estonia are heavily dependent on the alliance for their security. Facing possible Russian aggression, these small states have had to place a high priority on national defense. NATO, and thus, the United States, are key drivers of Baltic security. Likewise, Russian hybrid warfare activity is particularly frequent in the region, including, but not limited to, the cyber domain. Therefore, the policies outlined in this paper are of particular interest in Baltic capitals.

[52] https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE329/RAND_PE329.pdf

The inclusion of cyber assets alongside regular military operations is a crucial policy development. These components can increase the costs Russia must bear to conduct an attack, conventional or hybrid, in the Baltics. This change in the strategic calculus will affect decision-making in the Kremlin on what issues and what kinds of attacks are worth the cost. Likewise, the inclusion of offensive capabilities in U.S. policy adds to the risk Russia faces. Is a blackout in Tallinn worth a blackout in Moscow? By advertising that the United States and NATO are now not only able to retaliate in a manner that will be painful for Russia, but very well might do so, makes attacking Estonia far less attractive. This tightening of the screws will have two effects: Russia will be forced to understand that its actions may attract unwanted consequences, and Russia will be motivated to further develop its capabilities to obscure attribution. The latter effect – forced innovation – will also force innovation within the alliance, or else NATO will not be able to make good on its word, losing credibility. Until NATO meets that crossroads and makes a decision, however, these two policies will strengthen the credibility of NATO's deterrence posture in the cyber domain, positively impacting Baltic security.

Within the U.S. National Cyber Strategy, two other components are critical for the Baltics. The first of these is the stated priority on improving attribution of cyberattacks, imposing consequences, and neutralizing their effects. A focused effort on these crucial areas will provide a positive impact on the overall security of Lithuania, Latvia, and Estonia. By deterring hybrid warfare activities in the cyber

domain, the United States and NATO policies will bolster the overall security of the Baltics across multiple domains, from military security to societal security to energy security.

Likewise, the United States' stated commitment to build cyber capacity will further help the overall defense posture in the Baltic region. While Estonia is a leader in cyber defense, Latvia and Lithuania have lagged behind. If the United States makes good on its promise to build allies' cyber capacity with Lithuania and Latvia, this will improve not only those countries' readiness in the cyber domain, but also interoperability, streamlining crisis response.

## Conclusion

The United States' and NATO's cyber policy innovations over the last decade have responded to the growing sophistication and complexity of the threat environment in the cyber domain, particularly from state actors. Changes such as the adoption of offensive cyber instruments within the overall defense posture and allowing the use of cyber capabilities alongside other tools in multiple domains will create a more difficult strategic calculus for Russia in the Baltics and the rest of NATO's Eastern Flank. For Lithuania, Latvia, and Estonia, these changes are welcome improvements to the overall deterrence posture in the region, contributing to greater peace, stability, and security. These policy changes will have a variety of effects, most of them positive, but

only so long as the United States and its allies make good on the strategies set forth.

# Public-private partnerships

## Baltic developments in the EU framework

*Olevs Nikers*

While cyberattacks still remain among the primary business risks, competence and instruments to strengthen cyber security are sometimes hijacked by public sector bodies. Among the main issues is a lack of awareness about cybersecurity concerns for commercial organizations. Usually the knowledge about how to maintain cybersecurity remains within narrow circles of the government and national security community. As commercial security services frequently are unfamiliar with government experience, so government agencies are unfamiliar with the realities of today's private sector environment.[53]

### Public-private partnership framework in the EU

Cybersecurity is also a fundamental element for building trust, which is essential to the digital economy as well. Yet, the market supply for information and communication technologies (ICT) security products and services in Europe remains very fragmented, making it difficult for European companies to compete on the national and global level, and, for European citizens and enterprises to have access to viable technology. Thus, it is essential to encourage industry to

[53] How to build a public-private cybersecurity partnership for the modern era, https://www.weforum.org/agenda/2020/07/why-its-time-for-a-new-era-of-public-private-cybersecurity-partnerships/

supply more secure solutions and stimulate their take-up by enterprises and citizens.[54]

For that purpose, in its Digital market strategy for Europe of 6 May 2015, the Commission announced that in the first half of 2016 it would launch a public-private partnership on cybersecurity in the area of technologies and solutions for online network security. On 5 July 2016 it published a decision to establish the public-private partnership. The public-private partnership is to be instrumental in structuring and coordinating digital security industrial resources in Europe. The aim is to stimulate the European cybersecurity industry by bringing together industrial and public resources to improve Europe's industrial policy on cybersecurity, focusing on innovation and following a jointly-agreed strategic research and innovation roadmap; helping build trust among Member States and industrial actors by fostering bottom-up cooperation on research and innovation; helping stimulate cybersecurity industry by aligning the demand and supply for cybersecurity products and services, and allowing the industry to efficiently elicit future requirements from end-users; leveraging funding from Horizon2020 and maximizing the impact of available industry funds through better coordination and better focus on a few technical priorities; providing visibility for European R&I excellence in cybersecurity and digital privacy. The public-private partnership builds on the strategic research agenda in the area of secure ICT, developed by the Network and Information Security Platform as published in September 2015.

[54] PUBLIC-PRIVATE PARTNERSHIPS FOR CYBERSECURITY, https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-public-private-partnerships-for-cybersecurity

In 2013 European Commission presented the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace is the first strategic document on the European level which referred only to the cybersecurity sets a high priority for the public-private partnership within the cyber security domain.[55]

The Cybersecurity Strategy points out achieving cyber resilience as a strategic priority, and it was recognized that the effective cooperation between public authorities and the private sector is absolutely crucial. “Information and communications technology has become the backbone of our economic growth and is a critical resource which all economic sectors rely on. It now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport; while many business models are built on the uninterrupted availability of the Internet and the smooth functioning of information systems”. Most of these systems are under the private sector control, so for the governments protecting the cooperation with the industry is absolutely crucial. The Strategy encouraged Europe-wide discussions that initially started with the Commission’s 2009 communication on Critical Information Infrastructure Protection, about the need for private-public cooperation in the field of cybersecurity.

By the end of 2017 The European Union Agency for Cybersecurity (ENISA) has conducted a study on Cooperative Models for

[55] EU Cyber Security strategy: An open, safe and secure Cyberspace https://ec.europa.eu/home-affairs/what-is-new/news/news/2013/20130207_01_en

Public-private partnership and Information Sharing and Analysis Centers (ISACs), collating information on best practices and common approaches.[56] According to this study, building trust between public-private, private-private and public-public entities has been considered as one of the biggest challenges of public-private partnership and the cultural dimension was named as one of the most important determinants of the way that public-private partnerships are being established, developed and operated in Europe. Due to cultural differences, there is no universal scenario on how to create a successful public-private partnership; a model followed in one country will not necessarily fit another.

Other challenges that are named in this report are lack of human resources in both the public and private sector; insufficient public sector budget and resources that fail to meet the private sector's expectations; the establishment of a common level of understanding and dialogue between the public and private sector; promotion of the concept of public-private partnership among Small and Medium Enterprises (SMEs) and lack of leadership and legal basis.

"The main principles for setting up a public-private partnership ecosystem in Europe are to provide adequate human resources, as well as a legal basis of cooperation. It is also important to ensure open communication between public and private sector", as stressed in the ENISA Report.

[56] ENISA. Public Private Partnerships (PPP): Cooperative models, November 2017

Engagement in the process of Small and Medium Enterprises (SMEs) building is also crucial, since they are the backbone of the European economy. ENISA made a few recommendations on how to set up and run a public-private partnership: Motivation for the private sector to participate should be a priority when establishing a public-private partnership; the participants should agree to a legal basis when creating a public-private partnership; public institutions should lead the public-private partnership or the national action plan for public-private partnership; public-private partnerships should invest on internal private-private and public-public collaboration; public-private partnership participants should invest on open communication and a pragmatic approach towards building a public-private partnership, The representatives of the government should be allowed to participate in the meetings with non-disclosure agreement.

According to the ENISA study, there are multiple reasons for public-private partnership which are economic interests, regulatory requirements, public relations and social interests. Economic interests are the most common reason to establish a public-private partnership in Europe as it forms the most common motivation for the private sector to participate. Regulatory requirements for public-private partnerships are created as the implementation of a specific law whenever required and public administration decides that a public-private partnership framework will be the best way to do it. This covers mostly the case of crisis management or emergency law. Mostly this type of law deals with public-private partnership in general, not only in the field of cybersecurity.

In the case of public relations the government lets the private sector provide input to new legislation, as well as working together to develop a national cybersecurity strategy. For the private sector, the motivation lies in networking with the government and other private entities that share knowledge.

Social interest as a driving force for public-private partnership usually bears the motivation to discuss cybersecurity issues widely in the state, and set cybersecurity high on the political agenda. For the industry, the importance lies in promoting cybersecurity in general, so that the market could evolve without interruption.

Essentially, for private sector public-private partnership is import for several reasons, in particular it grants access to public funds, gives opportunity to influence national legislation and obligatory standards; access to public sector knowledge and confidential information (EU legislation, fighting cybercrime), and provides assurance that the products delivered through public-private partnership are of good quality, as it is guaranteed by the government.

For the public sector, benefits from public-private partnership lies in better understanding of Critical Infrastructure Information Protection (CIIP) and industry in general; possibility to create synergies between different initiatives of private sector, as well as it provides access to private sector resources (e.g. valuable experts), which makes it is easier to set up standards and good practices.

For public sector and private entities both, gains from the public-private partnership lies in sharing knowledge, experiences and good practices; mutual assistance to achieve resilience in the cyber ecosystem; increase the trust between public-public, private-private and public-private partnership allows to meet different people and get to know them; and finally, it allows to have better information and proactive attitude in case of crisis getting direct and credible contacts with other organizations.

Challenges and gaps within public-private partnership are related to the lack of human resources in both the public and private sector. Insufficient allocation of human resources in the development and evolution of public-private partnerships is considered as a major challenge according to the ENISA study. Also, insufficient public sector budgets and resources fail to meet the private sector's expectations. Governments often do not provide enough money for the development of public-private partnership.

The establishment of a common level of understanding and dialogue between the public and private sector is difficult to succeed within public-private partnership as different organizations use "different language". Lack of common perception on things can create misunderstandings that are difficult to handle and solve.

Also promotion of the concept of public-private partnership is undone among SMEs, which usually do not have enough resources or relevant experience to participate in public-private partnership.

Lack of leadership and legal basis is another challenge for successful public-private partnership within the cyber security domain.

**Public-private partnership challenges in the Baltics**

Lack of connection of cyber competence among the public and private sector is still an issue in the Baltic countries. Shota Gvineria, a lecturer in the Baltic Defence College pointed out that Estonia has made greater progress in building successful partnerships within the cyber security domain, compared to Latvia for example and this is another cross sectoral vulnerability. “Public sector will never be able to compete with the private sector attracting more talent within the field, this is a story of how you can develop stronger capacity, filling gaps of vulnerabilities so you need more brain and talent to address these challenges”, stressed Mr. Gvineria.

As it was reflected in the Baltic Security Strategy Report[57], Baltic States as a whole could utilize more institutionalized exchange of experiences and lessons learned in improving basic cyber-hygiene skills across public and private sectors. Moreover, public-private partnership within the cyber security domain is lacking both institutionally and practically. Cooperation with think tanks, tech startups, and other related groups will need to be considered and utilized to improve this domain. More intensive public-private partnership on cybersecurity awareness, training and exercise initiatives according to the Baltic Interoperability report is one of the

[57] Baltic Security Strategy Report, 2019

most important tasks for the upcoming years within the cybersecurity domain.

In general, lack of common educational approaches and limited state capacity are still an issue which undermines success in public and private partnering within the cyber security domain in the Baltic States. Estonia, thanks to its tremendous efforts at researching and contributing to the securitization of the cyber domain, has advanced the furthest not only within the Baltic region but globally as well.

Baltic countries are moving forward with the overall building of educated professionals in the field of cybersecurity. While this may be effective for each individual state's domestic goals, there is clearly a possibility here for better information exchange within the academic level and other private entities.

For Latvia, information exchange which allows engaging with private sector actors, is being exercised through Strategic Communications Centre of Excellence. Practice within this collaboration shows that direct expertise and strategies on handling disinformation and manipulation of algorithms can be provided within social media platforms from a technical perspective of information communication technology - an informational basis for the Ministry of Defense's national whole-of-society defensive approach.

Lithuania, for example has used data provided by the Energy Security Center of Excellence (ENSEC COE) to create a project that evaluates cyber risks concerning the operation of the Central

Europe Pipeline System (CEPS) and has proposed recommendations on improving the safety and availability of CEPS which is a good example of public-private partnership for cyber security within the energy security domain.

Estonia has established an organizational structure capable of rapid response to attacks and it has changed legal framework, so as all the vital services to be maintained a minimal level of operation if they have been cut off from the Internet. The measures taken by Estonia have established it as the highest-ranked European country when it comes to cybersecurity, and also provides a high rate of engagement of the private entities.

Increased security standards in regard to persons who have physical access to parts of infrastructure as well as inclusion private partners in the physical penetration tests within exercises are also of high importance to state security. For instance, the Stuxnet virus exploited physical weaknesses in systems to spread and cause considerable damage. Therefore, the Baltic State governments could actively practice a “bottom–up” approach, involving both state and private parties in joint exercises.

The main goal of these exercises should be to secure physical Internet infrastructure as well as carry out penetration testing (pentesting) on public networks and public-private critical infrastructure such as hospitals, telecommunications networks and banks.

As it was noted in the Baltic Interoperability report, cyber exercises, conducted by public entities have primarily focused on data protection during crisis situations; whereas, core physical infrastructure, upon which telecommunication and energy distribution networks rely, have only recently been included within live-fire exercises.

Regarding the cooperation of private and state organizations, the example of pentesting can be utilized in the public-private partnership domain. For example, the telecommunication providers in Lithuania, Estonia and Latvia could participate in joint drills with the CERTs as the governmental bodies and even utilize the special training environment popularized by IBM in Tallinn. This would serve to not only contribute to the protection of physical infrastructure but also to establishing common practices among specialists in the region.

There is also a dimension of cross border cooperation within the public-private partnership of the cyber security domain where currently three key sectors are left out: energy, banking and telecommunications. While cyber protection within energy security domain is managed through Transmission System Operators (TSO) and existing version of exchange of TSOs provides an environment for quick identification and mitigation of security disturbances and challenges in the online environment, it lacks informational collaboration with state CERTs, thus forcing them to singlehandedly tackle problems that could otherwise be handled cooperatively.

Banking sector is the second type of infrastructure with potential security vulnerabilities. Attacks in this area are mainly conducted by non-state actors for whom the primary interest lies in rising financial benefits. Thus, if the economic sector of a country is vulnerable, lack of cross border cooperation which also includes private entities, allows a malicious actor to execute the same attack in neighboring countries' associated banks.

Finally, the rise of the 5G debate, highlights the future importance of data security and critical infrastructure impacted by telecommunications. According to the Baltic Interoperability report, it requires a sustainable and cautious policy approach taken by the Baltic governments regarding supply chain security, engaging private entities in collaborative activities focusing on minimizing the spillover effect in case of a cyber-attack.

Majority of current initiatives and exercises are primarily being carried out within the frameworks of NATO and the EU, making it necessary to look deeper at the level of public-private partnership at the national level.

According to the Baltic Interoperability report, governments in the Baltic countries are in competition for skilled personnel with private firms, which provide IT operators with better wage options. Dozens of different programming languages, as well as multiple approaches to penetration testing and protecting data and infrastructure are in place. As a result, governmental institutions require an ever increasing number of professionals who are able to provide either

technical, legal or policy expertise with regard to the cyber domain. This lack of personnel capacity has become a major issue for Baltic State governments, including when it comes to boosting cooperation.

Despite the rapidly developing sphere of cybersecurity, the aforementioned lack of expertise in the public sector negatively impacts new regional initiatives or degrades maintenance of already-existing systems and networks. This requires further government involvement in cyber hygiene initiatives aimed at both publics, and private sector, as well as policymakers, with the aim to develop general understanding of possible threats and necessary actions to be taken regarding operations of ICT devices.

## Coronavirus and Cybersecurity

### Changes in the Cyber Threat Environment in Estonia, Latvia, and Lithuania

*Franklin Holcomb*

Over the past 18 months of pandemic, many existing trends in societal and threat-actor behavior online have been exacerbated creating a dangerous situation in which individuals, businesses, and states have found themselves underprepared to maintain their cyber security. Coronavirus has played a large part in driving this increase, primarily by increasing the use of e-services worldwide. As more and more individuals, private organizations, and governments were forced to take their leisure, business, and communication online the number of paths for and targets of cyber-attacks grew significantly. With more targets available, and more means to take advantage of them, cyber criminals and hostile state actors alike have more opportunity to exploit, disrupt, distort, and sabotage targets of their choice worldwide ranging from civilians, the state, to even society itself.

On NATO's Eastern flank, Estonia, Latvia, and Lithuania have historically frequently been targeted by hostile nation state actors in cyberspace. For over a decade, major Russian, or

Russian-orchestrated, cyber-attacks have caused massive societal disruption, economic turmoil, and security breaches on targets from the Black Sea to the Baltic Sea. This has led to an increased awareness of the risks posed to state and society by hostile actors in cyberspace across the region. Despite this, they were not shielded from the cyber impacts of Coronavirus. Hostile cyber actors, functioning both reactively and proactively to the pandemic, were driven to build on existing operations aimed at compromising the personal or national security of targets across the region. Cyber-criminals attempted to exploit a wave of disinformation and fear to profit from the pandemic. Hostile states took more of their activities to meet social-distancing and quarantine requirements. Some state-linked cyber actors increasingly targeted hospitals and medical facilities, while others attempted to spread disinformation related to the pandemic. The impact of these operations was not felt uniformly across the region, with Estonia reporting relatively minor impact and Lithuania reporting significant shifts, yet the sudden arrival of the pandemic put systems, cyber security agencies, and IT experts across the region to the test.

Coronavirus is beginning to come to an end. It can be hoped that many of the uncomfortable changes to personal and professional lives across the world may soon come to an end. It can also be hoped that the relative threat posed by hostile cyber actors will decline as more and more potential targets take their lives off their computers and into the real world. However, this sudden health crisis has demonstrated the importance of good personal

cyber-hygiene to individuals and the importance of sound cyber-security policy to the state. While it is true that no system will ever be secure and that no state will ever be able to make their society invulnerable to cyber-exploitation, it is equally true that investment in raising awareness of cyber threats in society and developing sound defense policies are key steps in the process of increasing national cyber security.

## The Pre-Covid Cyber Threat Landscape

Countries across Eastern Europe, prominently including Estonia, Latvia, and Lithuania, have been targets of anti-Western states for years and have developed extensive experience in dealing with hostile cyber actors. This experience has shaped regional thinking towards cyber security prior to the pandemic. Hostile intelligence agencies have conducted a wide range of operations including targeted attacks achieving traditional intelligence objectives such as extracting information but have also coordinated major operations aimed at causing widespread disruption and chaos in society.[58] Hostile states, prominently including the Russian Federation, have also made great efforts to distribute disinformation across the region aimed at sowing suspicion of the state and distrust between states. Meanwhile, cyber crime has posed a serious threat to private individuals and businesses in the region. The risks posed by hostile

[58] Holcomb, F. (2020). Countering Russian and Chinese Cyber-Aggression. Center for European Policy Analysis.
https://cepa.org/countering-russia-and-chinese-cyber-aggression/

cyber activity have been multiplied in the Baltic due to the region's strategic location and the openly aggressive geopolitical objectives of the Russian Federation.

Of all the threats faced by the Baltic states, the Russian government and government-linked cyber actors are the most severe. This is due to its wide set of tools ranging from economic and political pressure to direct military force against neighbors that it perceives as insufficiently compliant, thereby interfering in its objective to regain influence or control over former-Soviet space. A serious cyber attack against many countries in the West could be an embarrassment or allow a hostile state access to sensitive or classified data. However, a major cyber-attack in the Baltic could easily be prelude to a conventional military operation. This dynamic has made it all the more important for Estonia, Latvia, and Lithuania to increase the cyber-resilience of their societies while improving state capacity to respond in times of crisis, a process they have been actively engaged in for years. Edvinas Kerza, a former Deputy Defense Minister of Lithuania, emphasized that Lithuania's realization if hostile cyber actors conducted sufficiently effective disruptive attacks a war could be lost "before you fire a single bullet" motivated Lithuania's prioritization of improving its cyber defenses.[59]

Given the myriad and frequently overlapping cyber threats faced by Estonia, Latvia, and Lithuania all three countries have taken

[59] Ibid.

important steps in recent years to modernize their cyber defenses and innovate cost-effective methods to improve national and regional cyber resilience. Estonia stands out as the most experienced of the three given their years of building and securing an expansive e-governance system, though Latvia and Lithuania have also taken important steps to secure their national cyberspace in recent years. Policies implemented by the three Baltic states include:

*Cyber Militias:* All three of the Baltic states have created auxiliary cyber units in their national militias. These militias, the Estonian Kaitseliit, the Latvian National Guard, and the Lithuanian Riflemen's Union, are non-professional military formations intended to be mobilized during a time of national crisis to supplement state capacity. Their cyber units allow patriotically minded civilian cyber security professionals to commit free time to supporting state cyber objectives during peace time and directly supplementing state cyber operations in a time of crisis. These units also help erode the formal and informal barriers between state and civilian cyber security institutions.[60]

*Data Embassies*: Having previously faced some of the most serious attacks in the region, the government of Estonia created so-called "Data Embassies" in order to ensure government continuity in times of crisis. In practice, these embassies servers located in other

[60] Ibid.

countries which store and are regularly updated with state data. However, Estonia gave these servers the status of embassies and as such they benefit from the myriad rights enjoyed by embassies and are fully under Estonian jurisdiction. Estonia's data embassy project is intended to ensure that the government would be able to resume operation using data from the embassies if a hostile cyber attack denied access to, or destroyed, Estonian government data. In a more dangerous scenario, the Estonian government intends the data embassies to serve as backups in the event that the government were to temporary lose control of some of its territory in Estonia and lose access to its servers. [61]

*Training Centers:* All three of the Baltic states have prioritized the creation of international training and research centers to improve regional, and alliance-wide, cyber security and counter-disinformation practices. Such institutions include the NATO StratCom Center of Excellence and the Baltic Center or Media Excellence in Riga, the NATO Cooperative Defense Center of Excellence (CCDCOE) in Tallinn, and the Kaunas Cyber Security Center in Lithuania. All of these organizations have provided important research on evolving cyber threats and, most importantly, provide international experts the opportunity to work closely together to study cyber threats.[62]

[61] Ibid.

[62] Ibid.

Despite these and other important steps, no system or country is fully secure from hostile cyber action. This is particularly true of the Baltic states who face continued pressure, particularly from nation-state linked actors. Since the beginning of the Coronavirus pandemic, the threats facing the region have evolved and challenged all three of the Baltic states.

**Coronavirus and Its Regional Impacts**:

Coronavirus has played a major role in shaping the cyber threat environment throughout 2020, including in Estonia, Latvia, and Lithuania. Coronavirus led to significant spikes in cyber activity by both nation state and criminal cyber groups across the region. Impacts on each of the countries were not uniform, with differences likely attributed to differences in experience in cyber defense and societal cyber hygiene. Estonia reported relatively little change in the cyber threat environment while both Latvia and Lithuania warned that their systems had come under increasing pressure over the course of the pandemic. It is unclear whether these shifts will outlive the Coronavirus pandemic. However, given global trends towards increasing digitalization, it is likely that many of the new realities are here to stay. These distinctions in the impact of covid point to the importance of investment in cyber security, in terms of improving both state and societal capacity, in order to ensure NATO and European states are prepared to manage other real-world crisis with serious consequences in cyberspace.

### *Coronavirus' Impact on Online Activity*

Estonian, Latvian, and Lithuanian governments and societies responded to the Coronavirus pandemic in a similar manner to most countries, leading to a large increase in online activity. Indeed, for much of the pandemic regular life was taken online, thus increasing the amount of vulnerable data. Friends, families, and coworkers all took their normal interactions online. Meanwhile, many companies and governments struggled to find methods to make online workplaces secure. In particular, companies have struggled with ensuring that their employees secure their home devices, creating vulnerabilities for hostile cyber actors to exploit.[63] The Latvian State Security Service (VDD) summarized the shift in social-technological dynamics thus far in the pandemic in four points. Firstly, given the increase in online activity, many people used new technologies or software that might have unknown vulnerabilities that hostile cyber actors could exploit. Secondly, the increased use of personal devices might introduce vulnerabilities due to poor cyber hygiene. Thirdly, that Coronavirus presented a new and effective method to conduct phishing attacks. Fourthly, that the work of system administrators has become more difficult as they have to rapidly

[63] Melbarzde, L. (2021). Cybersecurity: "The strongest protection is well-trained employees." LSM.
https://eng.lsm.lv/article/features/features/cybersecurity-the-strongest-protection-is-well-trained-employees.a400826/

adjust to meet workplace requirements without compromising security.[64]

The increase in potentially valuable, and often imperfectly secured, data online has led to an increase in cyber incidents across Europe. These attacks have not only become more frequent but, in many cases, more sophisticated as cyber actors used social dynamics and fears caused by coronavirus to improve the effectiveness of their tools. Hackers have increasingly used social engineering as a method to gain access to key information. According to Europol, criminal hackers have used the pandemic to "attack vulnerable people" using numerous methods prominently including "phishing and online scams." These methods have often been enhanced by the spread of fake news related to Coronavirus, which increases the likelihood of potential targets engaging with dubious material embedded with malware by cyber criminals.[65] Meanwhile, ransomware attacks targeting public and private organizations, particularly those using Remote Desktop Protocol (RDP) services have become more frequent and severe.[66] The Lithuanian State Security Department (VSD) warned that the increase in remote work

[64] Annual Review for 2020 (2021). Latvian State Security Service.

[65] (2020) Covid-19 Sparks Upward Trend in Cybercrime. Europol. https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime

[66] (2020) Internet Organized Crime Threat Assessment. Europol; Welscher A. (2021) More than a virus: pandemic and online security in the Baltic states. LSM. https://eng.lsm.lv/article/economy/business/more-than-a-virus-pandemic-and-online-security-in-the-baltic-states.a399930/

and use of electronic services has increased the cyber-espionage threat.[67]

Over the course of the pandemic, there were three primary trends in changes to the cyber threat landscape. Firstly, hostile intelligence and espionage activities aimed at obtaining information or disrupting society. Secondly, hostile disinformation campaigns aimed at exploiting the covid pandemic. Thirdly, cyber criminality aimed at exploiting the heightened online presence for financial profit in societies across the region. These trends were not uniformly felt across the region, or at least have not yet been.

***Intelligence and Espionage**:*

Hostile states continued their traditional cyber operation against Estonia, Latvia, and Lithuania throughout the pandemic, however the Baltic states reported distinct shifts in hostile cyber intelligence behavior. Hostile states such as Russia and China have adjusted to the realities of the pandemic resulting in notable shifts in their operations including a shift towards online recruitment and a shift to targeting Coronavirus-related health infrastructure and research facilities. These shifts are not likely to long-outlast the pandemic, however their rapid emergence as a result of the pandemic

[67] National Threat Assessment 2021. (2021). State Security Department of Lithuania. https://www.vsd.lt/wp-content/uploads/2021/03/2021-EN-el_.pdf

illustrates the importance of ensuring all sectors of society are prepared to face cyber-attacks.

*New Methods:* Lockdowns and social distancing in the past year in the Baltic forced hostile intelligence agencies to shift their methods of intelligence collection and their methods of recruitment. The Latvian State Security Service (VDD) noted that coronavirus has complicated many traditional methods of collecting intelligence, increasing the relative importance of cyber intelligence, and warned that this trend is likely to increase in coming years.[68] Meanwhile, the Estonian Internal Security Service (KAPO) observed that Russian intelligence services, though initially reluctant to acknowledge the impact of coronavirus on their traditional methods of conducting their activities, had shifted recruitment efforts online.[69]

*New Targets:* The Coronavirus pandemic increased the strategic importance of medical facilities and medical research facilities worldwide, making them more attractive targets for cyber criminal groups and for hostile states. The Lithuanian VSD warned that in 2020 Russian-linked groups "conducted cyber-attacks against Lithuania's high-ranking decision makers, public institutions in the domains of foreign affairs, national security, and education."[70] They also accused the Russian-linked APT29 of attempting to use

[68] Annual Report for 2020. (2020) Latvian State Security Service (VDD)

[69] Estonian Internal Security Service Annual Review for 2020-2021. (2021) Estonian Internal Security Service.

[70] National Threat Assessment 2021. (2021). Lithuanian State Security Service. https://www.vsd.lt/wp-content/uploads/2021/03/2021-EN-el_.pdf

Lithuanian IT infrastructure to conduct cyber-attacks on other countries who were working to develop a vaccine against Coronavirus.[71] Latvian VDD echoed these concerns and warned that other states were attempting to exploit gaps in Latvian cyber defenses to use Latvian infrastructure as a "platform to coordinate attacks in other countries."[72] VDS warned that the Lithuanian National Public Health Center and the Klaipeda's Seamen's Hospital had been targets of cyber-attacks.[73]

*New Threat:* Over the course of the pandemic China has emerged as not only an increasingly significant actor in Baltic cyber space but also one with unfriendly intentions towards countries in the region. Chinese intelligence services do not behave as openly aggressively as their Russian counterparts. Instead, Chinese government hackers and disinformation units have preferred a more subtle approach to achieving their goals. National intelligence agencies across the region have begun to raise the alarm over Chinese intentions. In 2020, the Latvian VDD emphasized that Chinese intelligence viewed Latvia as a "platform for obtaining information about processes in NATO and the EU."[74] The VDD warned that there was increased activity of Chinese intelligence services "regarding the changes of China's public image in the context of the

[71] Ibid.
[72] Latvian State Security Service (VDD) Annual Report for 2020. (2021). Latvian State Security Service.
[73] National Threat Assessment 2021. (2021). State Security Department of Lithuania. https://www.vsd.lt/wp-content/uploads/2021/03/2021-EN-el_.pdf
[74] Latvian State Security Service (VDD) Annual Report for 2020. (2021). Latvian State Security Service.

Covid-19 pandemic… China's intelligence and security services were monitoring public opinion and targeting individuals who expressed opinions undesirable to China."[75]

Meanwhile, the Lithuanian VDS observed that Chinese government corporations and government entities were attempting to gain access to critical Lithuanian IT infrastructure by offering competitive bids to develop and install equipment.[76] VDS warned that these efforts posed serious long-term threats and would, if successful, allow China to 'carry out intrusive cyber operations, including the expropriation of data and knowhow, and would build its potential to undermine critical infrastructure in case of crisis."[77] It is likely that China will continue to attempt to increase its regional influence in coming years and involve itself in the development of regional IT infrastructure.

***Disinformation:***

Disinformation and traditional cyber security are frequently artificially put into different silos and viewed as distinct problem sets. This view ignores the reality that, in many cases, disinformation and hacking operations have overlapping objectives and can

[75] Ibid.

[76] Ibid.

[77] Ibid.

supplement one another. The amount of disinformation spread online worldwide soared over the course of the pandemic, including in Estonia, Latvia, and Lithuania. The Latvian VDD emphasized that the "rapid spread of conspiracy theories and their usage in various population groups… was one of the most visible side effects" of the efforts to combat the pandemic.[78] Much of this information was 'home grown,' however hostile states also contributed to the increase in disinformation in the public space. The VDS warned that in 2020 there were "18% more disinformation attacks than in 2019.[79]

Hostile government, prominently including Russia, used disinformation around pandemic to advance existing strategic objectives. The Lithuanian VDS warned that "foreign actors concurrently employ disinformation and cyber manipulations against Lithuania and its allies. Such operations aim to weaken transatlantic ties, sow discord in society and undermine public trust in state institutions."[80] In April 2021, the European Union accused Russia of orchestrating an information operation intended to "undermine and fragment the common European approach of securing vaccine supplies."[81] However, the pandemic has not been the primary topic of all online disinformation campaigns and some actors attempted to

[78] Ibid.

[79] National cybersecurity status report for the first time encompasses a perspective broader than just of the Ministry of National Defense. (2021). Kam.lt

[80] National Threat Assessment 2021. (2021). State Security Department of Lithuania. https://www.vsd.lt/wp-content/uploads/2021/03/2021-EN-el_.pdf

[81] Cook L. (2021) EU report takes aim at Russia over vaccine fake news. AP News. https://apnews.com/article/european-union-russia-europe-fake-news-coronavirus-d12316c1e6c21fe2f1a450e8f387dbac

use the pandemic as a method to improve the effectiveness of existing disinformation campaigns. The Russian Federation has been linked to numerous disinformation operations in previous years aimed at sowing distrust in NATO, including operations in which hackers facilitated the spread of disinformation by gaining access to and posting false information on numerous websites.[82] In March 2020 as the pandemic began to take hold in Europe, a disinformation operation targeting Lithuania aimed to make the Lithuanian Armed Forces appear to prioritize NATO operations over public health.[83] Disinformation can have various effects on a target, depending on the specific objectives of the campaign. However, the Coronavirus pandemic has demonstrated how domestic and foreign actors both will flood the online information space with disinformation during a crisis leading to decreased trust in the state and often increasing citizens' vulnerability to cyber criminals.

***Cyber Criminality**:*

Cyber-crime remains the most common threat online and has done widespread damage to national economies and the global economy over the course of the pandemic. Estonian, Latvian, and Lithuanian

[82] Welscher A. (2021). More than a virus: pandemic and online security in the Baltic states. LSM.
https://eng.lsm.lv/article/economy/business/more-than-a-virus-pandemic-and-online-security-in-the-baltic-states.a399930/

[83] Balciunas A. (2020) Coronavirus-linked cyber-attack targets Lithuanian defense minister. LRT.
https://www.lrt.lt/en/news-in-english/19/1153504/coronavirus-linked-cyber-attack-targets-lithuanian-defence-minister

cyber spaces have not been isolated from these global trends. As citizens of the Baltic states began to self-isolate and companies and governments across the region began to implement work from home policies, the number of cyber incidents increased. Vice-Minister of Defense of Lithuania Margiris Abukevicius observed that there is a "very obvious" correlation between the increase in cyber incidents in Lithuania and the start of the lockdown.[84] Meanwhile, the Estonian Information System Authority (RIA) warned that in 2020 there had been a "record number of phishing, distributed denial-of-service (DDos) attacks, Emotet malware, and cyber attacks targeting government ministries."[85] The global increase in cyber extortion, including ransomware and threats to launch Distributed Denial of Service (DDoS) attacks unless a ransom was paid, also impacted Estonia, Latvia, and Lithuania.[86]

The three Baltic states had some natural advantages which partially shielded them from some of the more severe criminal attacks. According to Baiba Kaskina, the General Manager of Latvian CERT, these include their relatively small market size, relatively large populations who communicate primarily or only in their local languages, and lack of legacy payment methods such as SMS

---

[84] (2021) Cyber Security report: Lithuania detects growth in attacks, online child exploitation. LRT. https://www.lrt.lt/en/news-in-english/19/1383234/cyber-security-report-lithuania-detects-growth-in-attacks-online-child-exploitation

[85] RIA yearbook: Cyber Criminals took advantage of COVID-19 Fears. ERR. https://news.err.ee/1608168793/ria-yearbook-cyber-criminals-took-advantage-of-covid-19-fears

[86] Welscher A. (2021). More than a virus: pandemic and online security in the Baltic states. LSM. https://eng.lsm.lv/article/economy/business/more-than-a-virus-pandemic-and-online-security-in-the-baltic-states.a399930/

banking. However, Kaskina also emphasized that, particularly in Latvia, the “lack of cyber security experts in the public sector” has been an especially difficult problem.[87] However, other vulnerabilities make the countries potentially attractive targets. These include imperfect cyber hygiene among segments of the population and the relatively common use of Russian which makes many common attacks, particularly using social engineering, by Russian-speaking criminal groups worldwide easier.

The pandemic has seen a significant increase in ransomware attacks, particularly targeting Remote Desktop Protocol (RDP) services.[88] Many of these attacks have been brute-force attacks, aimed at using various tools to guess common login information and gain access to potentially valuable accounts or data. Data published by Kaspersky labs warned that Lithuania, Estonia, and Latvia are “among the top 10 countries that are likely to experience RDP brute-force attacks.”[89] Phishing remains a common method of attack, which is often supplemented by disinformation that makes some people more likely to engage with dangerous material online.

[87] Melbarzde, L. (2021). Cybersecurity: “The strongest protection is well-trained employees.” LSM. https://eng.lsm.lv/article/features/features/cybersecurity-the-strongest-protection-is-well-trained-employees.a400826/

[88] Welscher A. (2021). More than a virus: pandemic and online security in the Baltic states. LSM. https://eng.lsm.lv/article/economy/business/more-than-a-virus-pandemic-and-online-security-in-the-baltic-states.a399930/

[89] Welscher A. (2021). More than a virus: pandemic and online security in the Baltic states. LSM. https://eng.lsm.lv/article/economy/business/more-than-a-virus-pandemic-and-online-security-in-the-baltic-states.a399930/

Over the past year and a half, cyber-criminals, potentially with links to foreign governments, have turned their attention to hospitals and medical institutions to exploit the pandemic by targeting hospitals and other healthcare institutions, aiming to extract ransom.[90]

**Conclusion:**

The Coronavirus pandemic has been an incredibly challenging time for the world. Millions have died, national economies are weakened, friends and families have been separated, and many feel that lives have been put on hold. However, Coronavirus' impact on cyber space has been significant as well. We are all more online than ever before, as is potentially valuable data. Hostile actors ranging from cyber criminals to nation states have adjusted and built on their operations in cyberspace to exploit these new dynamics. These dangerous changes have made increased state-state cooperation in cyber space all the more critical in terms of responding to specific threats as well as increasing resilience in general.

We cannot know what the next crisis will be. While this crisis has led to an increase in attacks on medical institutions, the next crisis might easily involve energy companies, international institutions, or any other sector of society. We must be proactive in analyzing the impact of the Coronavirus pandemic on cyber security. There are

[90] National Threat Assessment 2021. (2021). State Security Department of Lithuania. https://www.vsd.lt/wp-content/uploads/2021/03/2021-EN-el_.pdf

few cyber threats that only threaten one individual, organization, or country. Therefore, we must work together to ensure collective cyber security and increase our preparedness for the next crisis. To learn the right lessons from coronavirus, Western states should commit increased resources in coming years to not only the analysis and assessment of existing and emerging threats, but also what threats and cyber actions hostile actors online might take against the West in the event of global crisis or catastrophe. By doing this and learning from each other, states in the Trans-Atlantic community can improve their ability to address rapid changes in cyberspace such as those driven by the Coronavirus pandemic. These efforts must be matched with efforts by Western states and societies to improve societal resilience to cyber-attack by promoting cyber hygiene and increasing awareness of the dangers posed by hostile actors online if the West hopes to minimize the impact of hostile cyber action when the next global crisis takes place.

## Conclusions

The importance of Baltic States with regard to cybersecurity can be recognized on several accounts. On the one hand, the highly developed network infrastructure has paved the way to commercial and electronic public service developments that are consistently competitive not only in a regional, but also in a global setting.

At the same time, the geopolitical significance of the three states for international organizations, multinational companies and regional security stakeholders make the key role of cybersecurity a double-edged sword. As much as the Baltic experience serves as lessons learned for the EU, NATO and the U.S., any Baltic failures in the race for cybersecurity impact not only their constituent societies, but their allies as well. This may be increasingly pushed by their strategic opponents.

Whereas Baltic states are among the smaller members of NATO, the Alliance overshadows all other states and their bloks. So cybersecurity is a preferred domain to defeat an adversary slowly over time without fighting, as none of the opponents could match the allied resources outright. The membership of the Baltic States in NATO and the EU can also provide two goals at once for those countries which wish to influence policy outcomes in a target country via cyber means.

Looking at the NATO framework, the Baltic cyber resilience may benefit from additional regulation in terms of internal policies as well as international law that the allies may shape collectively. On the one hand, additional clarity on legitimate attribution and response to cyber attacks would certainly decrease the time required for NATO to decide on a particular reaction. On the other hand, unanimity between allies on certain principles may serve as a basis for developing customary international law to justify responses chosen by NATO or its individual members. The inclusion of cyber assets alongside regular military operations increase the costs opponents must bear to conduct an attack, conventional or hybrid, in the Baltics. This change in the strategic calculus will affect decision-making on what issues and what kinds of attacks are worth the cost. Likewise, the inclusion of offensive capabilities in the U.S. policy adds to the risk any opponent faces.

Additional regulation may limit symmetric response options for the Baltics or NATO, however the allied disagreement on developing collective offensive capabilities in conjunction with the track record of their strategic opponents in carrying out cyber attacks leads to the conclusion that the Alliance would not lose the most as a result of such a regulation. It may provide the grounds for attributing responsibility and providing a legal mechanism to solve claims for damages. This would be currently limited to diplomatic channels and mostly unproductive due to the obvious disinterest in accepting any liability.

As useful as the Tallinn Manual is, the lack of a binding nature for the included principles and criteria is a major drawback, so a concerted action by the Baltic States may put it in force at least in part and at least in a regional setting to start with. Regulations on collective economic and legal sanctions against the initiators of cyber attacks may serve as an alternative and politically less controversial first step in establishing a clear avenue of response. This may also be preferable to automatic counter striking, as that always contains a risk of exposing own vulnerabilities to the opponent.

Within NATO, the Baltic States have to initiate the discussion on whether the North Atlantic Treaty and other binding documents are up to date with the progressive importance of cybersecurity. Any changes to the said treaty may be too controversial politically, and the established ambiguity may actually prove to be useful for operational purposes, yet it is in the best interests of the Baltic States to not leave this for clarification when the next incident or crisis is already present.

Both NATO and EU can have an increasing role in awareness campaigns that educate citizens on proper cyber security, preventing wide scale damage. As such damage may be expected to have an impact on both security and economy, and affect social stability, it is important for these organizations to cooperate in their efforts to avoid duplication of resources with regard to this emergent

and complex threat. As noted by Olevs Nikers, there is both social and industry interest to have the services and markets develop uninterruptedly, however the governments are not in a position to outcompete the private sector for top talent, so public-private partnerships have to be considered for achieving cybersecurity objectives and it may be easier to do so from a multinational setting.

The coronavirus has brought about new cybersecurity issues beyond health care. The increasing use of electronic public services has gone hand in hand with ICT solutions being a more or less successful, yet certainly fundamental component of governmental response to the pandemic. The lack of a proactive stance by the Baltic governments on matters of cyber hygiene increases the risks of individual and national cyber-exploitation. It applies both in terms of cyber crime and also with regard to the vulnerability of critical infrastructure that societies are progressively reliant on, during the pandemic and likely after it as well.

## Baltic Security Foundation

The editors of this book have founded the Baltic Security Foundation to promote Baltic security and defense. This international non-governmental organization has been based in Riga, Latvia since 2019. The Foundation gathers experts on Baltic regional security from Europe, Asia and the Americas. The Foundation team provides situational assessment and recommendations on regional security that serve the public awareness and policy debate, decision making and evaluation.

The primary focus of the BSF activity is the Baltic Sea region within the Euroatlantic framework. The most recent project carried out by the BSF team, the Baltic Security Strategy Project, resulted in three international publications - the Baltic Interoperability Report, the Baltic Security Strategy Report, as well as the book “Baltic Sea Security: Regional and Sectoral Perspectives”. All reports are available online to contribute to the research and debate as much as possible.

Furthermore, the BSF has facilitated Baltic field visits of regional security researchers and experts from Western Europe, the United States, Brazil and Japan. BSF also provides guest lectures, seminars, research guidance, internships and networking for young leaders across the world seeking to specialize in the Baltic regional studies.