M. Górka, *Cyber deterrence policies of the Baltic states in the years 2016–2023*, „Rocznik Instytutu Europy Środkowo-Wschodniej" 22 (2024), z. 1, s. 45-66, DOI: https://doi.org/10.36874/RIESW.2024.1.3

Marek Górka*

Cyber deterrence policies of the Baltic states in the years 2016–2023

Polityka odstraszania cybernetycznego państw bałtyckich w latach 2016–2023

Abstract: Since spring 2014, political decision-makers and analysts have been engaged in a lively debate on the geopolitical confrontation between Russia and its neighbours. Following the Russian aggression against Ukraine, Estonia, Latvia, and Lithuania quickly became the focus of international attention. The article examines the evolution of the cybersecurity environment within the context of cyber deterrence policy. The main objective of the work is to identify the strategies adopted by small states when their security assurances are challenged by a powerful neighbour. An analysis of documents and cybersecurity concepts can serve as an explanation of the deterrence policies of the Baltic states.
Keywords: deterrence policy, cybersecurity, cyber security strategy, cyber defence, Baltic states, Russian threat
Streszczenie: Od wiosny 2014 roku decydenci polityczni oraz analitycy angażują się w ożywioną debatę na temat geopolitycznej konfrontacji między Rosją a jej sąsiadami. Po rosyjskiej agresji na Ukrainę, Estonia, Łotwa i Litwa stały się szybko centrum zainteresowania międzynarodowego. Artykuł koncentruje się na ewolucji środowiska cyberbezpieczeństwa w kontekście polityki odstraszania cybernetycznego. Głównym celem pracy jest zidentyfikowanie strategii, jakie przyjmują małe państwa w obliczu kwestionowania swoich gwarancji bezpieczeństwa przez potężnego sąsiada. Analiza dokumentów oraz koncepcji cyberbezpieczeństwa może posłużyć jako wyjaśnienie polityki odstraszania państw bałtyckich.
Słowa kluczowe: polityka odstraszania, cyberbezpieczeństwo, strategia cyberbezpieczeństwa, cyberobrona, państwa bałtyckie, zagrożenie rosyjskie

* Associate Professor, Koszalin University of Technology, ORCID: https://orcid.org/0000-0002-6964-1581, e-mail: marek_gorka@wp.pl.

Introduction

The main objective of this article is to interpret the perspective of the Baltic states in the area of cybersecurity policy. Cyber operations have become a modern manifestation of political warfare. Therefore, this article explores how states experiencing this threat perceive the phenomenon and what preventive actions they take. This research area fits into the well-known deterrence theory in the literature.

The article describes the deterrence policy carried out by small states in the face of a large neighbour based on the provisions found in strategic documents and intelligence reports, which define and indicate the threat posed by Russia's pursuit of interests in the cyber domain.

How states perceive digital threats not only reveals the most common threats but also reflects the subjective expression of their concerns, which is manifested in the way political decision-makers pay particular attention to specific security areas and allocate a certain amount of financial resources to defence infrastructure.

The purpose of the research analysis is to seek answers to the question: how do small states, with limited resources, maintain their security? Since many small states, including the Baltic states, lack significant military power, they are forced to seek other strategies for assurance or ways to influence other states[1]. Hence, it is understandable that small states have long been interested in promoting and strengthening international norms[2]. Such entities have certain characteristics that make them suitable for establishing norms[3]. Small states turn away from neutrality in favour of their presence in a larger organisation providing security.

In this article, we will examine this issue by analysing the attempts made by the Baltic states to establish norms related to cyber security. As small states feel threatened, especially by the use of digital tools by a stronger neighbour, they introduce norms to strengthen their secu-

1 M. Elman, *The Foreign Policies of Small States: Challenging Neorealism in Its Own Backyard*, "British Journal of Political Science" 1995, vol. 25, no. 2, pp. 175–199.

2 A. Kuczyńska-Zonik, *The Securitization of National Minorities in the Baltic States*, "Baltic Journal of Law & Politics" 2017, vol. 10, no. 2, pp. 32–36; M. Finnemore, K. Sikkink, *International Norm Dynamics and Political Change*, "International Organization" 1998, vol. 52, no. 4, pp. 887–917.

3 L. Goetschel, *Neutrals as brokers of peacebuilding ideas?*, "Cooperation & Conflict" 2011, vol. 46, no. 3, pp. 312–333.

rity and reinforce their national interests as a counterbalance to Russian influence[4].

This article focuses on the limitations and possibilities of building deterrence policy in the field of cybersecurity by small states. The intention of this work is to fill a gap in the literature and provide valuable insights into the process of norm and practice creation in the area of deterrence policy. This work is based on studies analysing the role of small states.

Analysing the discourses present in strategic documents and intelligence reports allows for a clearer understanding of how the security issues of the Baltic states have become more significant in NATO strategy, and subsequently, how these previously peripheral entities in international politics have begun to influence a broader NATO agenda.

The analysis in this article seeks to answer the question: what should be done to increase the credibility of the deterrence strategy of the Baltic states and other NATO countries, and to avoid aggression from Russia? The second aim of this study is to demonstrate that, despite the natural limitations of small states, these entities can serve as powerful means of advancing national interests at the international level through the promotion of norms.

To illustrate changes in the rhetoric of deterrence policy related to cybersecurity, this study decided to narrow the selected case to the years 2016–2023. These dates were chosen due to the instability following the annexation of Crimea in 2014 and the Russian invasion of Ukraine in 2022. The Baltic states were selected for analysis because they have structural similarities as small, Eastern European states, sometimes also called peripheral, bordering Russia. These similarities make them good candidates for examining NATO membership as a key variable.

4 M. Crandall, I. Varov, *Developing Status as a Small State: Estonia's Foreign Aid Strategy'*, "East European Politics" 2016, vol. 32, no. 4. pp. 405–425; R.B. Pedersen, *Bandwagon for Status: Changing Patterns in the Nordic States Status-Seeking Strategies?*, "International Peacekeeping" 2018, vol. 25, no. 2. p. 218; M. Melander, H. Mouritzen, *Learning to Assert Themselves: Small States in Asymmetrical Dyads – Two Scandinavian Dogs Barking at the Russian Bear*, "Cooperation and Conflict" 2016, vol. 51, no. 4. pp. 447–466; P.V. Jakobsen, J. Ringsmore, H.L. Saxi, *Prestige-seeking Small States: Danish and Norwegian Military Contributions to US-led Operations*, "European Journal of International Security" 2018, vol.3, no. 2, pp. 256–277.

The article is structured as follows: The first section includes a theoretical analysis of concepts such as small states, peripheral states, and deterrence policy in both conventional (traditional) and cybernetic approaches. The second part contains a section focusing on the theory of security policy of the Baltic states. This section describes the most important events and processes characterising the relations between Lithuania, Latvia, and Estonia, and the Russian Federation. The third section provides an analysis of the cybersecurity strategies and intelligence reports of the Baltic states. The research analysis of these documents will also describe progress in the development of strategies and policies in creating deterrent measures in relation to cybersecurity.

1. Cyber Deterrence Policy

In the face of evolving threats, the Baltic states are directing their attention towards strengthening their own political, economic, and military stability[5]. Upon joining the EU and NATO in 2004, they sought refuge, benefiting from the advantages and protection these organisations offer. However, despite these benefits, constantly emerging security threats, including cyber threats, challenge their ability to defend themselves effectively.

A powerful state in terms of military, economic, social, or territorial aspects is generally perceived as a threat by smaller states. This stems from the described material asymmetries and historical experiences[6]. Hence, it is understandable that small states often make decisions based on past threats[7]. The Baltic countries perceive Russia as a threat, largely due to their experiences over the past two centuries when these countries were part of the Russian Empire and the Soviet Union, during which they were compelled to undergo processes of Russification and Sovietization.

One way of emphasising and safeguarding their own independence and sovereignty on the international stage is through a policy of deterrence, which, in the case of the Baltic states, involves the fol-

5 J. Hey, *Small States in World Politics: Explaining Foreign Policy Behavior*, London 2003, pp. 2–3.
6 C.L. Glaser, *Realism*, [in:] A. Collins (ed.), *Contemporary Security Studies*, New York 2010, pp. 15–33.
7 A. Wivel, K.J.N. Oest, *Security, profit or shadow of the past? Explaining the security strategies of microstates*, "Cambridge Review of International Affairs" 2010, vol. 23, no. 3, pp. 429–453.

lowing actions: first, emphasising fundamental values directly related to sovereignty; second[8], invoking international organisations and norms to protect these fundamental values; and third, forming alliances to strengthen their identity and sovereignty[9].

At this point, it is worth referring to theoretical research that defines deterrence as a state action involving an attempt to convince the opponent to refrain from using violence, either by threatening retaliation or thwarting the opponent's operational plans[10]. Retaliation can be carried out by both the target country and its allies, ensuring credibility, international stability, and security. The would-be aggressor is convinced by other actors that aggression entails high costs and unacceptable damages, which outweigh the potential gains from conflict or aggression[11]. A fear of unnecessary consequences can deter the opponent and prevent or restrain some actions that have not yet begun but that the opponent may initiate[12]. Thus, deterrence entails costs, which may have material consequences or may take the form of loss of respect or credibility among the political environment. This may be based on a genuine fear of the possibility of undesirable events occurring or a sense of hopelessness in achieving the goal. Similarly, deterrence can be based on the belief that certain technology will be developed and become available for use. It may also rely on emotions associated with the difficulty of exiting a conflict. In this context, deterrence constitutes a psychological phenomenon that plays a significant role in the minds of political decision-makers. For the Baltic states, given the aggressive nature of the cyber environment, implementing a deterrence strategy is possible and may even prove to be the best option.

It is worth noting that not only fear of Russia serves as motivation, but also the desire to prove oneself as a loyal and credible ally forms

8 J.S. Levy, *Balances and balancing: concepts, proportions, and research design*, [in:] J.A. Vasquez, C. Elman (eds.), *Realism and the balance of power: A New debate*, Elman Prentice-Hall, 2003, pp. 128–153.

9 J. Robst, S. Polachek, Y. Chang, *Geographic proximity, trade and international conflict/cooperation*, Bonn 2006, https://docs.iza.org/dp1988.pdf [10.01.2024].

10 S. Von Hlatky, *Introduction: American Alliances and extended deterrence*, [in:] idem, A. Wenger (eds.), *The future of extended deterrence: The United States, NATO, and Beyond*, Washington 2015, p. 12.

11 K. Paulauskas, *On deterrence*, "NATO Review Magazine" 2016, http://www.nato.int/docu/review/2016/Also-in-2016/nato-deterrence-defencealliance/EN/index.htm [10.01.2024].

12 F.C. Zagare, *Deterrence theory*, Oxford 2013, pp. 1–27.

the foundation of deterrence policy in the case of the Baltic states. As Jakobsen[13] points out, this has prompted political decision-makers to work even harder to build a solid ally reputation in Washington. Specifically, in pursuit of such recognition, the Baltic countries have increased their defence spending to meet the NATO 2% target and contributed to the US-led anti-terrorism mission in Iraq. As Estonian President Kersti Kaljulaid noted, "the reputation image is very important for small countries"[14], and due to the high dependence on allies, countries like Estonia "constantly strive to behave as a reliable and predictable partner". As a result, they position themselves as staunch partners ready to pursue costly policies supporting their powerful ally.

In summary, the aim of deterrence is to prevent the opponent from taking certain actions. To achieve this, a state must clearly and credibly define what behaviours are undesirable and what the consequences of taking them will be. In particular, a clear and credible approach to deterrence can be effective, especially when it is possible to assign responsibility for actions. However, unclear consequences and vague threats can undermine the effectiveness of this strategy.

Deterrence strategy is becoming increasingly important in combating the growing cyber threat and in deterring key actors, both state and non-state, from conducting cyber attacks against state interests. The credibility of a state's response to cyber attacks is crucial for the effectiveness of deterrence. Without the ability to identify the attacker, the deterrence strategy loses its power and effectiveness.

Similar to traditional deterrence, the theory of cyber deterrence assumes that it is possible to deter malicious cyber actors by creating an expectation that the costs of retaliation will outweigh the benefits of malicious actions.

In the literature, it is often repeated that cyber deterrence requires the clear communication of consequences, costs outweighing perceived benefits, credibility of capabilities and determination, escalation

13 P.V. Jakobsen, J. Ringsmose, H.L Saxi, *Prestige-seeking small states: Danish and Norwegian military contributions to US-led operations*, "European Journal of International Security" 2018, vol. 3, no. 2, p. 275.

14 K. Kaljulaid, *On Estonian independence day in Tallinn 2017*, https://president.ee/en/official-duties/speeches/14740-president-of-the-republic-at-the-estoniatheatre-and-concert-hall-on-24-february-2017 [12.01.2024].

management, attribution skills, and policies defining when to "voluntarily attribute cyber operations"[15].

Joseph Nye argues that cyber deterrence depends on perception, attribution, uncertainty, and the risk of escalation, and should take into account entanglement and norms[16]. Will Goodman contends that examples from everyday life show that cyber deterrence is feasible, but challenges include attribution, anonymity, scalability, certainty, escalation, and clear signalling[17]. On the other hand, Michael Fischerkeller and Richard Harknett argue that the uniqueness of cyberspace makes deterrence below the threshold of the use of force unworkable[18]. Mariarosaria Taddeo points out that, due to the deterrent reasons, the nature of cyberspace is limited in terms of attribution, credible signalling, escalation, uncertainty of consequences, and proportionality[19]. Attribution, credibility, clear communication, scalability, environmental uncertainty, misconceptions, escalation, compromise risk, unintended consequences, and normative issues are recurring themes in the scholarly debate.

It is worth noting that in the case of harmful cyber activities targeting national interests, such as critical infrastructure, a credible and effective deterrence policy requires the imposition of higher consequences[20]. Offensive cyber capabilities are a way to impose costs on entities that are increasingly resilient to diplomatic, legal, or economic instruments. By leveraging offensive cyber capabilities, states can change the decisions of such entities regarding costs and benefits, while shaping international norms. Therefore, cyber deterrence means using offensive cyber capabilities to impose dramatic costs on entities

15 A. King, M. Gallagher, *United States of America Cyberspace Solarium Commission Report*, Washington 2020, pp. 26–34.

16 J.S. Nye, *Deterrence and Dissuasion in Cyberspace*, "International Security" 2016, vol. 41, no. 3, pp. 44–71.

17 W. Goodman, *Cyber Deterrence: Tougher in Theory than in Practice?*, "Strategic Studies Quarterly" 2010, vol. 4, no. 3, pp. 102–135.

18 M.P. Fischerkeller, R.J. Harknett, *Deterrence Is Not a Credible Strategy for Cyberspace*, "Orbis" 2017, vol. 61, no. 3, pp. 381–393.

19 M. Taddeo, *The Limits of Deterrence Theory in Cyberspace*, "Philosophy & Technology" 2018, vol. 31, no. 3, pp. 339–355.

20 J. Osawa, *The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?*, "Asia-Pacific Review" 2017, vol. 24, no. 2, pp. 116.

engaging in unacceptable actions. It exploits the relative advantages of cybercrime to compel retaliatory targets to defend everywhere, while simultaneously providing evidence of consequences, actors, and their actions. To curb the scope and aggressiveness of malicious cyber activities, costly reprisals are necessary.

In summary, cyber deterrence as a component of the security policy of the Baltic states, may provide opportunities to gain an advantage in the information environment. Cyber capabilities are a way to impose costs on entities that are less susceptible to diplomatic, law enforcement, or economic actions. However, it is worth noting that cyber deterrence seems to require a more coherent effort from both the state and society. Cyber threats are directed not only against the state but also against other entities whose security is crucial for the security of society as a whole.

The effectiveness of deterrence is greatly influenced by the vast number of potential actors, making the generation of defensive measures in cyberspace particularly complex[21]. This complexity creates challenges in determining what to protect and how to protect it, and makes responding to each individual breach increasingly difficult[22]. Another challenge in cyber deterrence is the lack of international norms, such as ineffective inter-state or inter-institutional cooperation, as cyber incident information is typically classified. At the interstate level, this may stem from the inability to discern correlated patterns of isolated incidents, as entities are reluctant to share information due to national security concerns – or simply because they are unsure what information to share. Conversely, commercial entities may be unwilling to provide relevant data to government agencies out of fear of compromising confidentiality and customer trust, which in turn can impact their revenues[23].

As such, approaching the creation of a true deterrent in cyberspace still requires clarification in many areas where there are currently too

21 S. Jasper, *Deterring Malicious Behavior in Cyberspace*, "Strategic Studies Quarterly" 2015, http://www.au.af.mil/au/ssq/digital/pdf/Spring_2015/jasper.pdf [14.01.2024].

22 E. Iasiello, *Is Cyber Deterrence an Illusory Course of Action?*, "Journal of Strategic Security" 2014, vol. 7, no. 1, p. 54.

23 L. Clinton, *Cyber Security Social Contract*, [in:] S. Jasper (ed.), *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*, Washington 2012, pp. 185–198.

many unexplored variables and poorly developed concepts, which often undermine the effectiveness of a state's cyber defence.

2. The evolution of security policy in the Baltic States: from periphery to central role

As this article focuses on the policy of the Baltic states, it is worth defining their common name, which characterises their nature as political entities, namely the term "small states". This term is used for entities in several cases: firstly, when they are unable to showcase their potential on a global scale; secondly, when they lack material resources that build their international status, such as population size, GDP, state area, or military strength; and thirdly, the perception and preferences of political decision-makers themselves[24].

The literature on the subject points out the main goals set by the authorities of small states, which include efforts to be noticed by larger powers in matters of international peace and security, meaning the desire to be publicly recognised as such by a major power. These states also strive for recognition by the international community as entities with high moral authority, which also translates into the position of a credible partner towards a stronger power[25]. Research also indicates that "the pursuit of status has always been a central element of the foreign and security policy of small states"[26].

While research on small states and their ambitions to achieve status in international relations is well-established, an area where research is just beginning to develop is cybersecurity policy, which in a way is independent of the physical characteristics that often determine a state's position in traditional terms.

Another important term used to describe the position of the Baltic states, found in academic literature or public discourse, is "peripherality". In light of current events, it may seem obvious that this term does not fully correspond to the Baltic states, which in recent years

24 C. Archer, A. Bailes, A. Wivel, *States and International Security. Europe and Beyond*, London 2014; G. Baldacchino, A. Wivel (eds.), *Handbook on the Politics of Small States*, Northhampton 2020, pp. 2–19.

25 B. de Carvalho, I.B. Neumann (eds.), *Small States and Status Seeking: Norway's Quest for International Standing*, London 2015, p. 2.

26 R.B. Pedersen, *Bandwagon for Status…*, p. 235.

have become important for the security strategies of European countries towards Russia, considering their proximity to the eastern borders of the EU and NATO.

Peripheries, perceived as places on the "margins", not only refer to those located at a distance from a given centre but are also imbued with social implications that may vary in different contexts[27]. The geographical positioning of the Baltic states on the eastern outskirts of NATO was of little significance in the post-9/11 era, when US political dominance focused its attention on the Middle East. However, the situation of Lithuania, Latvia, and Estonia on the outskirts of NATO, in the period preceding the crisis in Ukraine, was shaped by the minimisation of the influence of dominant NATO member states.

Due to changes in the global situation, mainly caused by Russia's aggressive policies, the Baltic states gained strategic, and consequently, greater significance for the Alliance. The reassessment of the importance and role of this region coincided with the views expressed by Kühn, who emphasised that "peripheries are not doomed to remain on the margins forever"[28]. As a result of Russia's annexation of Crimea, the geography of NATO's eastern borders did not change, which led to new significance attributed to the role of Eastern Europe's borders[29]. This change necessitated the adjustment of programs that emphasise equal priorities and develop material responses in Estonia and the Baltic Sea area to confront perceived threats from Russia.

Since regaining independence, relations between Russia and the Baltic states have encountered fundamental problems with military implications. The main issue was the geostrategic position of the Baltic states between Russia and the West. These states clearly expressed their intention to join NATO; however, ethnic tensions between Baltic and Russian communities also played a role in this situation.

There are three key issues generating political tensions between the Baltic states and Russia. First, the significant presence of Russian-speaking communities in each of these states, especially in Estonia

27 C.S. Browning, P. Joenniemi, *Contending discourses of marginality: The case of Kaliningrad*, "Geopolitics" 2004, vol. 9, no. 3, pp. 699–730.

28 M. Kühn, *Peripheralization: Theoretical concepts explaining socio-spatial inequalities*, "European Planning Studies" 2015, vol. 23, no. 2, pp. 367–378.

29 R. Legvold, *Return to cold war*, Malden 2016, pp. 152–154.

and Latvia, with both countries outnumbering Lithuania in this sense. The second notable issue is Russia's enduring and growing influence in the areas of science and media. Russian-speaking individuals and those sympathetic to Russia's ideology likely constitute a significant portion of Lithuania's academic community. Additionally, Russia exerts significant influence over television and radio programs in Lithuania and Latvia, particularly through cable services[30]. The third issue is Russia's direct or indirect influence on electoral processes in the Baltic countries. Russian organisations, including the government, have supported various political parties in these states. For example, during one election, Russian President Vladimir Putin indirectly offered his support to a specific political party in Latvia[31]. In 2004, former Lithuanian President Rolandas Paksas was accused of ties to criminal and political organisations in Russia after nearly two years in office. There are also allegations that the Russian intelligence agency played a significant role in the election of Riga Mayor Nils Ušakovs, who is the first ethnic Russian to hold this position[32].

The Baltic states are geographically situated in an area that connects Russia with Europe and is historically considered a region of uncertain stability. There is concern that history may repeat itself as Russia may take retaliatory actions in response to NATO's activity related to the crisis in Ukraine. The elites of the Baltic states propagate the belief that Russia may invade Ukraine and then turn its actions towards the Baltic region[33]. Russia appears to be seeking to regain influence in the Baltic states, which were once part of the Soviet Union. As a result, increased Russian activity in the region is observed, aimed at assessing NATO's reaction. These actions are perceived as an attempt to test the readiness of the United States and European coun-

30 A. Kuczyńska-Zonik, K. Sierzputowska, *Wpływy Rosji i Chin w państwach bałtyckich*, "Prace Instytutu Europy Środkowej" 2022, vol. 8, pp. 21–22, 34; N. Maliukevicius, *Russia's information policy in Lithuania: the spread of soft power or information politics?*, "Baltic Security & Defence Review" 2007, vol. 9, pp. 150–170.

31 N. Muižnieks, *Russian foreign policy towards "Compatriots" in Latvia*, [in:] idem (ed.), *Latvian-Russian relations: domestic and international dimensions*, Riga 2006, pp. 119–130.

32 *Latvia: Russia's playground for business, politics – and crime*, "The Guardian", 23 January 2013, https://www.theguardian.com/world/2013/jan/23/latvia-russian-playground [24.02.2024].

33 A. Kuczyńska-Zonik, K. Sierzputowska, *The Baltic States in the Face of Russian Aggression in Ukraine*, [in:] A. Kasińska-Metryka, K. Pałka-Suchojad (eds.), *The Russia-Ukraine War of 2022. Faces of Modern Conflict*, London 2023, pp. 41–59.

tries to support the most vulnerable allies[34]. Groups of Baltic states may be potential targets for traditional Russian expansionist policies[35].

The Baltic states are aware of the nature of the potential Russian threat, which may manifest in the form of asymmetric warfare, the use of intelligence services, economic instruments, and direct armed conflict. Examples of Russian aggression against Chechnya, Georgia, and Ukraine clearly indicate Russia's intentions towards its neighbours[36].

The Baltic states pay particular attention to strengthening their defence capabilities and ensuring cybersecurity. A comparative analysis of the investments made by these countries in the years 2016 and 2023 allows for a deeper understanding of the evolution of their security policies in the face of evolving challenges.

In 2016, Lithuania allocated 575 million EUR to its defence budget, with 115 million EUR earmarked for cybersecurity. By 2023, it had increased its defence budget to 1.83 billion EUR, with proportional spending on cybersecurity reaching 366 million EUR. Latvia invested 360 million EUR in defence in 2016, with cybersecurity expenditures amounting to 33 million EUR. By 2023, its defence budget had risen to 1.33 billion EUR, with 319.2 million EUR allocated to cybersecurity. Estonia, in 2016, invested 450 million EUR in defence, with 108 million EUR dedicated to cybersecurity. By 2023, it had increased its defence budget to 1.33 billion EUR, with a simultaneous increase in cybersecurity spending to 319.2 million EUR[37].

Analysis of this data reveals a noticeable trend of increasing investments by the Baltic states in defence and cybersecurity between 2016 and 2023. The increased financial commitment to these areas demonstrates the growing awareness of security threats by these countries and their determination to ensure effective defence in the digital age.

34 D. Takacs, *Ukraine's Deterrence Failure: Lessons for the Baltic States*, "Journal on Baltic Security" 2017, vol. 3, no. 1, pp. 1–10.

35 L. Zdanavičius, N. Statkus, *Strengthening Resilience of Lithuania in an Era of Great Power Competition: The Case for Total Defence*, "Journal on Baltic Security" 2020, vol. 6, no. 2, pp. 1–21.

36 M. Andžāns, V. Veebel, *Deterrence Dilemma in Latvia and Estonia: Finding the Balance Between External Military Solidarity and Territorial Defence*, "Journal on Baltic Security" 2017, vol. 3, no. 2, pp. 29–41.

37 Defense budgets of the Baltic Sea countries in the years 2016–2023. *The Military Balance 2016–2023*, https://www.iiss.org/publications/the-military-balance [24.02.2024].

Based on available data on defence spending, it is clear that the Baltic states not only benefit from the alliance but also actively participate in NATO's collective defence, as evidenced by a comparison of defence expenditures. Investments in defence were motivated by Russian aggression in Ukraine and a realisation of their own vulnerabilities. Preparing the armed forces for collective and territorial defence tasks has become the new policy focus. The Baltic states have implemented modernisation programs, focusing on both restoring combat readiness and strengthening cybersecurity capabilities.

3. Cybersecurity strategies of the Baltic States 2016–2023

In the realm of Baltic state politics, strategies are developed somewhat independently of each other, but under the pressure of various factors such as threats from Russia or membership in the North Atlantic Treaty Organization (NATO) and the European Union (EU), the mutual cooperation of political entities becomes necessary. This analysis also aims to identify specific threats related to current security discussions, and those visible in the official political narrative of the Baltic states. In an increasingly digital age, cybersecurity strategy becomes a crucial element in the field of security. The provisions in these documents not only require the Baltic states to be proactive in cybersecurity but also constitute part of the norm-shaping process.

A common denominator regarding deterrence policy development can be observed across all three strategies. The first aspect of these actions involves strengthening defensive capabilities in cybersecurity, as a state with strong defensive cybersecurity capabilities is presumably less attractive to potential aggressors. The second factor highlights the importance of international cooperation in combating cyber threats, as cooperating states have a greater ability to pursue perpetrators and respond to attacks. The third area of activity for the Baltic states is the prevention and combating of cybercrime. Preventive actions, such as employee education and cybersecurity awareness, can deter potential perpetrators by making it more difficult for them to carry out successful attacks. The strategy authors also emphasise the importance of maintaining defensive capabilities. They highlight the need for a rapid and effective response to cyber incidents, as this

demonstrates the state's determination to defend its resources and interests in cyberspace.

The Lithuanian *National Cybersecurity Strategy 2018* highlights the importance of routine and regularly updated training for public and private sector employees in cybersecurity. This approach aims to increase cybersecurity culture through education, which can deter potential cybercriminals from harmful actions[38]. The document authors point out the need for effective dissemination of information about the latest cyber incidents and factors increasing the risk of data breaches or susceptibility to cybercrime[39]. The strategy also includes sections addressing the concept of innovation, interpreted by the document authors as investment in scientific research, the development of new technologies, and services in the field of cybersecurity[40]. Together, these elements indicate an approach based on cybersecurity culture, education, and cooperation, aimed not only at increasing awareness but also deterring potential attackers by increasing the difficulty and risk associated with cybercrime.

The authors of the Latvian *The Cybersecurity Strategy of Latvia 2023–2026* discuss the observed increase in attacker activity, including scanning, vulnerability probing, phishing campaigns, and DDoS attacks[41]. This indicates a recognition of the need to deter these malicious activities. The strategy highlights two key entities, serving as the main tools in the country's cyber defence: The first is the National Cyber Security Centre (NCSC), which plays a central role in monitoring and responding to cyber threats, sharing threat information, and coordinating national cybersecurity efforts[42]. The existence of a dedicated cybersecurity agency reflects a commitment to deterring cyber threats through active monitoring and response. The second point is Security Operations Centers (SOCs), which host information systems of state institutions in data centres. This system is a crucial element of cybersecurity strategy because it provides real-time monitoring and incident

38 *National Cyber Security Strategy 2018*, pp. 12–13, https://kam.lt/en/cyber-security/ [15.01.2024].
39 Ibid., p. 13.
40 Ibid., p. 14.
41 *The Cybersecurity Strategy of Latvia 2023–2026*, p. 9, https://www.mod.gov.lv/en/nozares-politika/cybersecurity [16.01.2024].
42 Ibid., p. 11.

response capabilities[43]. Its operation strengthens the deterrence factor by signalling readiness to rapidly respond to cyber attacks. The strategy also emphasises EU-level initiatives such as the NIS2 Directive and the EU Cybersecurity Strategy[44], aimed at creating an effective and comprehensive cybersecurity management model by implementing EU cybersecurity regulations into national legislation to comply with EU standards.

In the Estonian *Cybersecurity Strategy Republic of Estonia 2019–2022*, there is a strong emphasis on building organisational structures responsible for maintaining the country's digital resilience. This strategy highlights the importance of international cooperation, cyber defence exercises, and research offered by the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), and has a strategic interest in promoting the development of the centre as an international organisation[45]. Collaboration with international entities is emphasised to legitimise the state's position, significance, and capabilities in cybersecurity[46]. The continuous development of capabilities in conducting cyber operations, including the ability to carry out retaliatory actions, is one of the key elements of Estonia's deterrence policy. Throughout the cybersecurity strategy, Estonia is portrayed as a pioneer in recognising the importance of cybersecurity, especially after the cyber attacks in 2007. The text underscores the importance of raising the level of cyber hygiene in government institutions and local governments, emphasising the need for knowledge and awareness of cybersecurity among public administration employees[47]. Estonia aims to play a leading role in NATO's cyber defence issues, which is a form of cyber deterrence, as it involves developing capabilities to defend against cyber threats and attacks. Estonia actively participates in cyber defence exercises such as "Locked Shields" and "Cyber Coalition"[48]. These exercises simulate cyber attacks and responses, contributing to the development of effective deterrence and defence

43 Ibid., p. 18.
44 Ibid., p. 19.
45 *Cybersecurity Strategy Republic of Estonia 2019–2022*, pp. 56–57, https://www.mkm.ee/en/e-state-and-connectivity/cyber-security/ensuring-states-cyber-security [14.01.2024].
46 Ibid., p. 35.
47 Ibid., p. 67.
48 Ibid., p. 60.

strategies. In summary, the above documents form a comprehensive strategy that not only enhances defensive capabilities in cybersecurity but also acts as a deterrent to potential attackers. The deterrence policy in the context of cybersecurity for Baltic states is based on increasing awareness, a readiness to respond, and international cooperation, creating more challenging conditions for cybercriminals and increasing the risk associated with cyber attacks.

4. Cyber deterrence in the context of intelligence reports

Analysis of intelligence reports provides valuable insights into the study of cyber deterrence in the Baltic states. Although there may be concerns that the full reality of cyber threats is incompletely presented in such documents, publicly available intelligence analyses serve as excellent complements to cybersecurity strategies and offer a much more current perspective for public institutions responsible for security on an international level.

The 2022 Lithuanian *National Threat Assessment* clearly indicates growing concerns from Lithuania and its Western allies regarding the actions of Russia and other authoritarian states. The text emphasises the increasing influence of China, Russia's aggressive actions in the region, cyber threats, and propaganda efforts by Russia and Belarus[49]. Russia is considered the greatest and potentially existential threat, with specific challenges arising from actions such as the migration crisis on the Lithuania-Belarus. Reports from previous years also referred to Russia as the main threat, highlighting its military buildup and activity in the region, including in Kaliningrad Oblast. Special tools posing a threat to the stability of the state include intelligence activities undertaken by Russia in Lithuania and cyber actions targeting critical infrastructure. Defining the tools of disinformation used by the Russian Federation is an important element. Intelligence documents, especially from the period 2016–2018, emphasise the threat posed by the growing role of Russian media in Lithuania, including

49 *National Threat Assessment 2022*, pp. 25–29, https://www.vsd.lt/en/threats/threats-national-security-lithuania/ [22.02.2024].

the development of the Sputnik channel[50]. This indicates Russia's efforts to spread its message and influence public opinion, posing a serious challenge to democratic states, which must strengthen their defence mechanisms against external interference. Documents also point to Russia's increased activity in cyber espionage, including the activities of the APT28/Sofacy group, which is linked to the Russian military intelligence service GRU[51]. This group employs more advanced methods such as spear phishing to gain access to information, suggesting that Russia is more interested in acquiring data in cyberspace.

Similarly to analyses from Lithuania and Estonia, Latvia's intelligence reports from the Latvian State Security Service from 2016 to 2023 are marked by an evolving perception of the Russian threat. Here are a few key observations: The first three reports from 2016, 2017, and 2018 seem to treat Russian actions as part of a broader set of challenges and threats to security, which include the spread of disinformation and political extremism[52]. Threats are perceived more generally and less focused on Russia. It is only in the reports from 2019 and 2020 that the growing threat from Russia is more strongly emphasised. Violations of international law, war crimes, and the violation of Ukraine's territorial integrity are noted. Russia is portrayed as a brutal political actor acting in contradiction to democratic values. The text also references Russia's hybrid actions aimed at shaping public opinion in favour of Russian imperial aspirations[53]. Documents from 2021, 2022, and 2023 continue to perceive Russia as an aggressor and violator of international law. The ongoing influence of Russian propaganda and information activities on Latvian society is also noted. In 2022, it was noted that the activity of the Latvian State Security Service (VDD) was focused on identifying threats and crimes that were difficult to prevent, such as hate speech and incitement to ethnic hatred[54]. There were also warnings about the actions of individuals sympathetic to the Kremlin, who were expressing support for war.

50 *National Threat Assessment 2018*, p. 13, ibid.
51 *National Threat Assessment 2017*, p. 25, ibid.
52 *Latvian Security Police. Annual Report for 2017*, p. 18, https://vdd.gov.lv/en/useful/annual-reports [12.02.2024].
53 *Latvian Security Police. Annual Report for 2020*, p. 8, ibid.
54 *Latvian Security Police. Annual Report for 2022*, p. 4, ibid.

In Estonian reports titled *International Security and Estonia* starting from 2016, the importance of cooperation with allies and partners in ensuring the security of Estonia and the Baltic region is emphasised. The reports contain a detailed analysis of threats from Russia, demonstrating efforts made by Estonian agencies to better understand the nature of these threats[55]. It can also be argued that this knowledge serves as an important tool for building cooperation with representatives of intelligence and counterintelligence services of Western European countries. Such knowledge is an excellent tool for enhancing readiness for deterrent actions. It is also worth emphasising that having detailed data builds Estonia's prestige in the international community.

The analyses note that Russia utilises so-called "patriotic hackers" during periods of crises or conflicts. These hackers work in favour of Russia and may conduct attacks on targets related to states or organisations that criticize Russia or are in conflict with it[56]. Specific Russian cyber groups are mentioned, such as APT28 (Sofacy/Fancy Bear), SNAKE (Turla), and APT29 (Cozy Bear/The Dukes), along with information about their links to Russian special services[57]. Earlier texts also indicated the activities of Russian groups but without providing specific names and associations.

The analysed reports clearly emphasise the need for defence against cyber attacks, strengthening cyber infrastructure, and international cooperation in cybersecurity. Intelligence analyses point to security threats to the Baltic states, particularly those associated with Russia, highlighting the need to prepare for various types of threats, including hybrid and informational ones. All documents underscore the importance of international cooperation in responding to common threats with other states and international organisations. Another important element is recognising Russia's actions as violations of international law and aggression, which is a common thread. The unity and solidarity of the Baltic states with Ukraine and other countries affected by Russia's actions is noteworthy, and in itself can be interpreted as a deterrent.

55 *International Security and Estonia 2022*, p.20. https://www.valisluureamet.ee/assessment.html, [12.02.2024].
56 *International Security and Estonia 2019*, p.48, Ibid., [12.02.2024].
57 *International Security and Estonia 2018*, p.53, Ibid., [12.02.2024].

Conclusions

The conclusion drawn from the analysis of the potential cyber capabilities of the Baltic states is neither simple nor one-dimensional. The process of building these capabilities is lengthy and complex, determined by various factors. Primarily, the Russian military threat is a common denominator in the cybersecurity policies of Lithuania, Latvia, and Estonia.

The conclusion from the analysis of the security policies of the Baltic states is that they seek to undertake a series of actions to strengthen their defence capabilities. An important step was the increase in defence spending, followed by accelerated modernisation. Another significant improvement is the rapid development of military infrastructure. The Baltic states have invested in military infrastructure at the national level and in cooperation with strategic partners through NATO and EU programs. The actions taken by the Baltic states aim to enhance their defence capabilities and strengthen regional security. Through international cooperation and investments in modern technologies and infrastructure, Estonia, Latvia, and Lithuania demonstrate readiness for the effective defence of their territory and the security of their citizens.

Deterrence is a complex issue that may involve various aspects, such as demonstrating defence capabilities, responding to attacks, or diplomatic efforts to deter potential adversaries from cyber actions. Deterrence policy in cybersecurity is a relatively new area and continues to evolve in response to changing cyber threats. Often, it is not traditional deterrence based on the threat of the use of military force, but rather deterrence based on other means aimed at discouraging potential aggressors. It is also worth emphasising that the strategies of the Baltic states primarily focus on building defence capabilities aimed at minimising the damage caused by cyber incidents.

References

1. Andžāns M., Veebel V., *Deterrence Dilemma in Latvia and Estonia: Finding the Balance Between External Military Solidarity and Territorial Defence*, "Journal on Baltic Security" 2017, vol. 3, no. 2.
2. Archer C., Bailes A., Wivel A., *States and International Security. Europe and Beyond*, London 2014.
3. Baldacchino G., Wivel A. (eds.), *Handbook on the Politics of Small States*, Northhampton 2020.
4. Browning C.S., Joenniemi P., *Contending discourses of marginality: The case of Kaliningrad*, "Geopolitics" 2004, vol. 9, no. 3.
5. Carvalho B. de, Neumann I.B. (eds.), *Small States and Status Seeking: Norway's Quest for International Standing*, London 2015.
6. Clinton L., *Cyber Security Social Contract*, [in:] S. Jasper (ed.), *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*, Washington 2012.
7. Crandall M., Varov I., *Developing Status as a Small State: Estonia's Foreign Aid Strategy'*, "East European Politics" 2016, vol. 32, no. 4.
8. *Cybersecurity Strategy Republic of Estonia 2019–2022*, https://www.mkm.ee/en/e-state-and-connectivity/cyber-security/ensuring-states-cyber-security [14.01.2024].
9. Elman M., *The Foreign Policies of Small States: Challenging Neorealism in Its Own Backyard*, "British Journal of Political Science" 1995, vol. 25, no. 2.
10. Finnemore M., Sikkink K., *International Norm Dynamics and Political Change*, "International Organization" 1998, vol. 52, no. 4.
11. Fischerkeller M.P., Harknett R.J., *Deterrence Is Not a Credible Strategy for Cyberspace*, "Orbis" 2017, vol. 61, no. 3, pp. 381–393.
12. Glaser C.L., *Realism*, [in:] A. Collins (ed.), *Contemporary Security Studies*, New York 2010.
13. Goetschel L., *Neutrals as brokers of peacebuilding ideas?*, "Cooperation & Conflict" 2011, vol. 46, no. 3.
14. Goodman W., *Cyber Deterrence: Tougher in Theory than in Practice?*, "Strategic Studies Quarterly" 2010, vol. 4, no. 3.
15. Hey J., *Small States in World Politics: Explaining Foreign Policy Behavior*, London 2003.
16. Hlatky Von S., *Introduction: American Alliances and extended deterrence*, [in:] idem, A. Wenger (eds.), *The future of extended deterrence: The United States, NATO, and Beyond*, Washington 2015.
17. Iasiello E., *Is Cyber Deterrence an Illusory Course of Action?*, "Journal of Strategic Security" 2014, vol. 7, no. 1.
18. *International Security and Estonia 2016–2023*, https://www.valisluureamet.ee/assessment.html [12.02.2024].
19. Jakobsen P.V., Ringsmore J., Saxi H.L., *Prestige-seeking Small States: Danish and Norwegian Military Contributions to US-led Operations*, "European Journal of International Security" 2018, vol. 3, no. 2.
20. Jakobsen P.V., Ringsmose J., Saxi H.L., *Prestige-seeking small states: Danish and Norwegian military contributions to US-led operations*, "European Journal of International Security" 2018, vol. 3, no. 2.

21. Jasper S., *Deterring Malicious Behavior in Cyberspace*, "Strategic Studies Quarterly" 2015, http://www.au.af.mil/au/ssq/digital/pdf/Spring_2015/jasper.pdf [14.01.2024].
22. Kaljulaid K., *On Estonian independence day in Tallinn 2017*, https://president.ee/en/official-duties/speeches/14740-president-of-the-republic-at-the-estoniat-heatre-and-concert-hall-on-24-february-2017 [12.01.2024].
23. King A., Gallagher M., *United States of America Cyberspace Solarium Commission Report*, Washington 2020.
24. Kuczyńska-Zonik A., Sierzputowska K., *The Baltic States in the Face of Russian Aggression in Ukraine*, [in:] A. Kasińska-Metryka, K. Pałka-Suchojad (eds.), *The Russia-Ukraine War of 2022. Faces of Modern Conflict*, London 2023.
25. Kuczyńska-Zonik A., Sierzputowska K., *Wpływy Rosji i Chin w państwach bałtyckich*, "Prace Instytutu Europy Środkowej" 2022, vol. 8.
26. Kuczyńska-Zonik A., *The Securitization of National Minorities in the Baltic States*, "Baltic Journal of Law & Politics" 2017, vol. 10, no. 2.
27. Kühn M., *Peripheralization: Theoretical concepts explaining socio-spatial inequalities*, "European Planning Studies" 2015, vol. 23, no. 2.
28. *Latvia: Russia's playground for business, politics – and crime*, "The Guardian", 23 January 2013, https://www.theguardian.com/world/2013/jan/23/latvia-russian-playground [24.02.2024].
29. *Latvian Security Police. Annual Report for 2016–2023*, https://vdd.gov.lv/en/useful/annual-reports [12.02.2024].
30. Legvold R., *Return to cold war*, Malden 2016.
31. Levy J.S., *Balances and balancing: concepts, proportions, and research design*, [in:] J.A. Vasquez, C. Elman (eds.), *Realism and the balance of power: A New debate*, Elman Prentice-Hall, 2003.
32. Maliukevicius N., *Russia's information policy in Lithuania: the spread of soft power or information politics?*, "Baltic Security & Defence Review" 2007, vol. 9.
33. Melander M., Mouritzen H., *Learning to Assert Themselves: Small States in Asymmetrical Dyads – Two Scandinavian Dogs Barking at the Russian Bear*, "Cooperation and Conflict" 2016, vol. 51, no. 4.
34. Muižnieks N., *Russian foreign policy towards "Compatriots" in Latvia*, [in:] idem (ed.), *Latvian-Russian relations: domestic and international dimensions*, Riga 2006.
35. *National Cyber Security Strategy 2018*, https://kam.lt/en/cyber-security/ [15.01.2024].
36. *National Threat Assessment 2016–2023*, https://www.vsd.lt/en/threats/threats-national-security-lithuania/ [22.02.2024].
37. Nye J.S., *Deterrence and Dissuasion in Cyberspace*, "International Security" 2016, vol. 41, no. 3, pp. 44–71.
38. Osawa J., *The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?*, "Asia-Pacific Review" 2017, vol. 24, no. 2.
39. Paulauskas K., *On deterrence*, "NATO Review Magazine" 2016, http://www.nato.int/docu/review/2016/Also-in-2016/nato-deterrence-defencealliance/EN/index.htm [10.01.2024].
40. Pedersen R.B., *Bandwagon for Status: Changing Patterns in the Nordic States Status-Seeking Strategies?*, "International Peacekeeping" 2018, vol. 25, no. 2.
41. Robst J., Polachek S., Chang Y., *Geographic proximity, trade and international conflict/ cooperation*, Bonn 2006, https://docs.iza.org/dp1988.pdf [10.01.2024].

42. Taddeo M., *The Limits of Deterrence Theory in Cyberspace*, "Philosophy & Technology" 2018, vol. 31, no. 3.
43. Takacs D., *Ukraine's Deterrence Failure: Lessons for the Baltic States*, "Journal on Baltic Security" 2017, vol. 3, no. 1.
44. *The Cybersecurity Strategy of Latvia 2023–2026*, https://www.mod.gov.lv/en/nozares-politika/cybersecurity [16.01.2024].
45. *The Military Balance 2016–2023*, https://www.iiss.org/publications/the-military-balance [24.02.2024].
46. Wivel A., Oest K.J.N., *Security, profit or shadow of the past? Explaining the security strategies of microstates*, "Cambridge Review of International Affairs" 2010, vol. 23, no. 3.
47. Zagare F.C., *Deterrence theory*, Oxford 2013.
48. Zdanavičius L., Statkus N., *Strengthening Resilience of Lithuania in an Era of Great Power Competition: The Case for Total Defence*, "Journal on Baltic Security" 2020, vol. 6, no. 2.