RESEARCH ARTICLE

Baltic States Cyber Security Policy: Development of digital capabilities in 2017–2022

Marek Górka

Faculty of Humanities, Politechnika Koszalinska, Koszalin, Polska, 75-343, Poland

Abstract

The Baltic Sea region is currently one of the tensest areas in Europe, with Russia potentially challenging the international order by provoking a new confrontation with the North Atlantic Treaty Organization (NATO). In this context, the Baltic States of Lithuania, Latvia, and Estonia are developing their cyber security capabilities, which provides an intriguing example of how small states with an aggressive neighbour can operate. The perceived threat is driving the development of cyber capabilities, and policymakers are prioritizing efforts to strengthen their digital capabilities. This article aims to examine the security challenges faced by the Baltic States in the digital environment and their strategies for enhancing digital capacity building competencies. Additionally, the article focuses on the Baltic States' efforts to build and strengthen cyber capabilities, which serve as the foundation for their cyber security policies. To accomplish this, data from the Digital Economy and Society Index (DESI) was utilized, employing research methods including quantitative, qualitative, and comparative analyses. This approach aimed to evaluate and compare the progress in digital capabilities among the Baltic States. Additionally, an analysis of strategic documents was conducted to gain insight into each country's perspective on cyber security and to identify opportunities for the development of this field in consideration of available resources. The findings emphasize the Baltic states' dedication to bolstering their cyber resilience, primarily motivated by the perceived threat from Russia. The study underscores the intricate relationship between socioeconomic factors and a nation's cyber capabilities. The conclusion drawn is that their endeavours to establish and enhance cyber capabilities constitute a pivotal component of their cybersecurity strategy, thus contributing to regional stability and NATO's collective defence.

Keywords

cyber security policy, Baltic States, digitalisation, digital potential, cyberpower

Corresponding author: Marek Górka (marek_gorka@wp.pl)

Author roles: Górka M: Conceptualization, Formal Analysis, Investigation, Methodology, Software, Validation

Competing interests: No competing interests were disclosed.

Grant information: The author(s) declared that no grants were involved in supporting this work.

How to cite this article:
For printed version: Górka Marek. "Baltic States Cyber Security Policy: Development of digital capabilities in 2017–2022". *Stosunki Międzynarodowe – International Relations* 59, (2023): 57–81. Printed 2023. https://doi.org/10.12688/stomiedintrelat.17684.1.

For online version: Górka M. **Baltic States Cyber Security Policy: Development of digital capabilities in 2017–2022.** Stosunki Międzynarodowe – International Relations 2023, **3**:15 https://doi.org/10.12688/stomiedintrelat.17684.1

Introduction

In recent decades, the Baltic States have prioritized improving their national defence to respond to security threats posed by Russia's aggressive policies. These reforms have primarily focused on professionalizing activities in strategy and adapting standards to meet European Union (EU) and North Atlantic Treaty Organization (NATO) requirements and criteria.[1] While Moscow has long considered the region part of its sphere of influence, the means of confrontation and pressure utilized by Russia have evolved.[2] Much of this action now occurs in the digital space and through it.

Threats posed by the dominant role of cybertechnology are increasingly becoming an argument for changing existing security policy models. The article presents the attitudes of the Baltic States towards the digital sphere and information technology, with the aim of broadening debates on the importance of cyber security for states, economies, and societies, thanks to new digital technologies.

Digitalisation has undoubtedly contributed to the growth of economies and the development of societies worldwide. However, a negative feature of this process is the enormous dependence of critical infrastructure on cyber technology, which can have a direct impact on the functioning of the state and its citizens. Cyber attacks, for example, can restrict access to state resources and undermine trust in public institutions. Building necessary cyber security capacity to protect societies from digital damage is one of the most pressing questions.

To contribute to the development of knowledge on cyber security policy, the article analyses the actions taken by individual governments to assess cyber-capability development attitudes and actions to improve the level of cyber security among the Baltic States. In this context, the actions of governments in enhancing cyber capabilities can be seen as a tool for building deterrence strategies to protect national security against cyber threats.[3]

Due to the increase in various forms of cyber threats and their potential to affect the well-being of countries worldwide, many governments have taken several initiatives to improve their cyber security posture. One of the main objectives of this article is to note the changes taking place in the defence preparedness of the Baltic States in the area of cyber security. Additionally, it is worth mentioning that although there is a heated debate on the impact of cyber capabilities on security policy, little research has been devoted to seeking answers to the question of why some states are better prepared for cyber threats than others.

[1] V. Veebel and I. Ploom, "Are the Baltic States and NATO on the right path in deterring Russia in the Baltic?," *Defense & Security Analysis* 35, no. 4 (2019): 406–422.

[2] A. Banka and M. Bussmann, "Uncomfortable neighbors: NATO, Russia and the shifting logic of military exercises in the Baltics," *Defence Studies* 23, no. 1 (2023): 1–24.

[3] A. Calderaro and A.J.S. Craig, "Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building," *Third World Quarterly* 41, no. 6 (2020): 917–938.

To provide a better understanding of how policy initiatives can support cyber capacity development efforts, an analysis of the Baltic States' cyber preparedness will be made based on selected 'Digital Economy and Digital Society Indicators (DESIs)'[4] developed by the European Commission regarding the cyber capabilities of EU countries. The article aims to provide the latest data and analyses concerning cybersecurity policy in the Baltic states. The goal is to facilitate an understanding of the changes and progress in digital capabilities that have taken place in the region from 2017 to 2022. By comparing data from previous years, it is possible to identify the evolution of approaches to the cybersecurity issue and to pinpoint potential challenges and opportunities in the future. Empirical data, especially those related to indicators such as DESI, the share of the ICT sector in GDP, gross domestic expenditure on research and development, and the number of reported patents in the field of cybersecurity, can indicate specific steps that have been taken in the realm of digital capabilities and the achieved outcomes. Furthermore, this analysis can shed light on areas still requiring reinforcement and unresolved issues. As a result of the conducted analysis, recommendations and conclusions will emerge, which might prove valuable for decision-makers, policymakers, and institutions dealing with cybersecurity. This comparative analysis of cyber security efforts at the level of specific countries can help assess and measure the readiness of cyber capacity development efforts. Additionally, the identification of different approaches to cyber security management can help define a specific state cyber security policy model.

The article also characterizes factors to analyse progress in cyber capacity building by examining strategic documents. This research perspective can be useful for analysing cyber security policy measures in response to the growing threat against the Baltic States. Based on the above-mentioned points, the aim of this paper is to discuss individual factors that can be considered as strategic strengths and noteworthy capabilities to strengthen the states' cyber defence.

The topic of the Baltic states directly relates to issues that have already been widely described and studied, namely the politics of small states. These entities possess limited resources, which hinder their influence on international policy and effective defence against external threats. Additionally, they are more susceptible to systemic instability. In the research of many scholars, traditional material indicators such as GDP, population, military potential, and territorial size are often used to determine the degree of state smallness.[5] Insufficient diplomatic and administrative resources are also pointed out.[6] However, other researchers emphasize the

[4] "The Digital Economy and Society Index (DESI)," accessed June 2, 2023, https://digital-strategy.ec.europa.eu/en/policies/desi.

[5] J. Corbett and J. Connell, "All the World is a Stage: Global Governance, Human Resources, and the 'Problem' of Smallness," *Pacific Review* 28, no. 3 (2015): 435–459.

[6] *Small States and International Security: Europe and Beyond*, eds. C. Archer, A.J.K. Bailes and A. Wivel (New York, NY: Routledge, 2014).

importance of new factors such as perception, image, reputation, international status, as well as foreign policy activity.[7] They argue that traditional definitions based solely on material indicators do not fully capture the reality that small states face in the contemporary world.[8]

The majority of research on small states focuses on security issues, yet this area is most often analyzed through the prism of political, military, and economic factors.[9] In this context, emphasizing digital potential as a factor of ensuring security allows capturing the actions of small states aimed at overcoming natural security limitations. Thus, it presents an opportunity for striving towards a level playing field on the international stage. Within this context, highlighting the role of digital potential as a key security-enabling element helps understand the nuanced actions undertaken by small states to overcome their inherent security constraints. As a result, such emphasis holds the potential to level the playing field for these states in the international arena.

Changes in the security environment, systemic challenges, and limitations stemming from geopolitical factors are prompting the Baltic states to seek new ways of ensuring security by harnessing cyber technologies. Contrary to previous theories suggesting that small states have limited resources to establish themselves on the international stage,[10] it is precisely these states that, through the utilization of cyber technologies, can achieve significant successes and strengthen their political standing. The main premise of this thesis is the growing correlation between the bolstering of small states' positions and their effective and efficient actions in the cyberspace arena. However, it is worth considering the concrete steps these states have taken to improve their defences that could prove useful in the event of a hypothetical cyber aggression from Russia. Additionally, it is important to assess whether the Baltic States are moving in the right direction in designing and reforming their national defence systems, given the analysis of national defence models in

[7] A. Wivel, "From Peacemaker to Warmonger? Explaining Denmark's Great Power Politics," *Swiss Political Science Review* 19, no. 3 (2013): 298–321; *Closing NATO's Baltic Gap*, eds. W. Clark *et al.* (Tallinn: International Centre for Defense and Security, 2016).

[8] B. Thorhallsson, "Studying Small States: A Review," *Small States & Territories* 1, no. 1 (2018): 17–34.

[9] A. Banka, "Neither reckless nor free-riders: auditing the Baltics as US treaty allied," *Journal of Transatlantic Studies* 20, no. 2 (2022): 161–183; *Small States and Security in Europe: Between National and International Policymaking*, eds. T. Weiss and G. Edwards (New York: Routledge, 2021); M. Crandall and M.L. Sulg, "Small states and new status opportunities: Estonia's foreign policy towards Africa," *European Politics and Society* 24, no. 2 (2023): 250–264; *Small Baltic States and the Euro-Atlantic Security Community*, ed. S. Sraders (New York: Palgrave Macmillan, 2021); *Small States and the New Security Environment*, eds. A.M. Brady and B. Thorhallsson (Springer Nature Switzerland AG, 2021); V. Veebel, "NATO options and dilemmas for deterring Russia in the Baltic States," *Defence Studies* 18, no. 2 (2018): 229–251; Veebel and Ploom, "Are the Baltic States and NATO," *Defense & Security Analysis*, 406–422.

[10] M. Crandall and C. Allan, "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms," *Contemporary Security Policy* 36, no. 2 (2015): 346–368.

Estonia, Latvia, and Lithuania. Have these states adopted similar or different approaches to their cyber defence? In the context of the lack of significant military power in these countries, it is worth considering whether the digital tools being used are sufficient to pursue state interests and strengthen security.

To build adequate cyber capabilities, states must meet the right criteria to achieve their cyber security objectives. This requires having both the right capabilities and a willingness to act in the digital area. In order to examine the level of digital capability of the Baltic States, data from the Digital Economy and Society Index (DESI) will be used. The study will use quantitative, qualitative, and comparative methods to provide a comprehensive assessment of digital progress among the countries studied.

After presenting data that illustrates the development of cyber capabilities in Lithuania, Latvia, and Estonia, this study aims to compare the changes occurring in each of these countries and across the Baltic region. This will be done based on a range of variables, including investment in cyber security, the capacity for technology assimilation by society, the economic and scientific potential of each country, and the number of patents filed in the field of cyber technology, among others. These diverse variables will enable the identification and assessment of various processes, which will in turn provide a more comprehensive characterization of each country's cyber security policy.

The following section of the paper will include an analysis of the most recent strategic documents to explore how the individual Baltic States perceive the concept of cyber security. This method will identify similarities and differences in approaches to solving specific problems and point to opportunities for cyber security development. These opportunities will be interpreted in the context of the resources that are crucial to the Baltic States' cyber capabilities.

Cybersecurity policy as an opportunity for small states

When examining the threats against the Baltic States, parallels to events in Ukraine naturally emerge. Since the Russian annexation of Crimea, there has been frequent speculation about whether the Kremlin authorities will take military action against the Baltic States. This concern has only intensified since the full-scale invasion of Ukraine in February 2022.

Security threats associated with Russia have been a major area of interest among military strategists and international policy analysts for many years. Most suggest that the Baltic States are potentially at risk.[11] The predictions of analysts and

[11] Veebel and Ploom, "Are the Baltic States and NATO," 406–422; A. Radin, *Hybrid Warfare in the Baltics: Threats and Potential Responses* (Santa Monica, CA: RAND Corporation, 2017).

public figures, including former NATO Secretary General Anders Fogh Rasmussen, who warned of the "high probability" of future Russian action against the Baltic States, also support these concerns.[12] The Baltic States represent a meeting point between Russia's political interests and NATO.

Russia is a major factor in the security agendas of the Baltic States, which feel vulnerable due to their small size and their proximity to a state that pursues an expansionist policy towards its neighbours.[13] The Kremlin uses a variety of methods, both overt and covert, as tools to implement its foreign policy, and it also employs massive disinformation campaigns and cyber attacks, which can be effective political instruments within the framework of hybrid warfare.[14]

As a result, the Russian threat to the territorial integrity and sovereignty of the Baltic States has become the centrepiece of their national security. Following the Russian aggression in Ukraine, the Baltic States have accelerated their efforts to enhance their digital defence capabilities. Baltic defence planners have been compelled to achieve long-term goals in a shorter timeframe.

While membership in international organizations such as the EU and NATO provides significant benefits and protection for states, new security threats are challenging their ability to protect themselves. Traditional territorial conflicts, while still present on the world stage, do not pose the same great threat to small states as they did during the Cold War.[15] However, small states remain vulnerable to new threats, such as cyber attacks and disinformation campaigns. Nevertheless, their ability to influence the world is increasing. The expansion of NATO and the EU also means that small states have the ability to influence some of the world's most influential organizations. Further reinforcing the importance of small states is digitalization, which has created linkages on a global scale where a threat to one state can affect many others.[16]

[12] A.S. Dahl, *Strategic Challenges In the Baltic Sea Region Russia Deterrence and Reassurance* (Georgetown University Press, 2018).

[13] G. Vitkus, "Changing Security Regime in the Baltic Sea Region," Working Paper (Vilnius, NATO Euro-Atlantic Partnership Council Individual Research Fellowship 2000–2002 Programme), accessed June 2, 2022, https://www.nato.int/acad/fellow/99-01/Vitkus.pdf.

[14] G. Simons, Y. Danyk and T. Maliarchuk, "Hybrid war and cyber-attacks: creating legal and operational dilemmas," *Global Change, Peace & Security* 32, no. 3 (2020): 337–342; C.K.G. Lutz, B.J. Lutz and J.M. Lutz, "Russian Foreign Policy Management and Manipulation with the Soviet Successor States," *Terrorism and Political Violence* 31, no. 1 (2019): 84–97.

[15] M. Ekengren, "A return to geopolitics? The future of the security community in the Baltic Sea Region," *Global Affairs* 4, no. 4–5 (2018): 503–519.

[16] D. McCrory, "Russian Electronic Warfare, Cyber and Information Operations in Ukraine," *The RUSI Journal* 165, no. 7 (2020): 34–44.

Sovereignty is always a primary existential goal for all small states.[17] This can refer to politics, economics, armed forces, and nowadays, also to digital capabilities ensuring stability in cyberspace. The changing international environment and the evolving nature of security, along with the systemic challenges and constraints posed by the geopolitical location and size of the Baltic States, are compelling policymakers to explore new ways to ensure their security, relying on the opportunities offered by cyber technology, among other things.[18]

The article contributes to the academic debate on the cyber security policies of small states and their impact on the external environment. Previous policy literature has highlighted that small states are vulnerable to traditional security challenges due to their limited diplomatic and administrative resources, as well as weak bargaining and military power.[19] Consequently, their ability to shape the international order is often limited.[20]

One of the main characteristics of the Baltic States' security is their limited resources to influence international policy or protect themselves from external threats, which makes them more vulnerable to systemic instabilities. A state's digital capabilities can therefore prove that legacy elements, such as strategic depth, are irrelevant.

The development of cyber security is an unquestionable principle for many states, making it a popular topic for security studies and international relations. States that neglect this space are consequently harmed by the actions of those actors who decide how to use their cyber capabilities. The effectiveness of a state's cyber security, which is essential for the defence of the economy and military communication and command, is directly dependent on its cyber capabilities. Given the defensive and offensive importance of cyber security, many states are taking steps to develop this capability.[21]

The importance of cyber security policy is often emphasized due to the increasing pressure on governments from the social, economic, and technological

[17] J.W. Lamoreauxa, "Acting small in a large state's world: Russia and the Baltic states," *European Security* 23, no. 4 (2014): 565–582; *Small states in Europe: challenges and opportunities*, eds. R. Steinmetz and A. Wivel (Farnham: Ashgate, 2010); K.S. Gleditsch and E. Gartzke, "Small and constrained vs. large and insular? Country size and the liberal peace," APSA 2010 Annual Meeting Paper, July 19, 2010; A.F. Cooper and T.M., Shaw, "The diplomacies of small states at the start of the twenty-first century: how vulnerable? How resilient," in *The diplomacies of small states: between vulnerability and resilience*, eds. A.F. Cooper and T.M. Shaw (New York: Palgrave-Macmillan, 2009), 1–18.

[18] N. Bladaitė and M. Šešelgytė, "Building a Multiple 'Security Shelter' in the Baltic States after EU and NATO Accession," *Europe-Asia Studies* 72, no. 6 (2020): 1010–1032.

[19] C. Archer, "Small states and the European Security and Defence Policy," in *Small states in Europe: challenges and opportunities*, eds. R. Steinmetz and A. Wivel (Farnham: Ashgate, 2010), 47–62.

[20] A.J.K. Bailes, "Does a Small State Need a Strategy?," Occasional Paper, Reikjavik, Center for Small State Studies Publication Series, 2009.

[21] A.J.S. Craig, R.A.I. Johnson and M. Gallop, "Building cybersecurity capacity: a framework of analysis for national cybersecurity strategies," *Journal of Cyber Policy* (February 21, 2023): 1–24.

environment to develop the ability to compete in this field.[22] When cyberspace and the processes within it are perceived as threats to national security, policymakers strengthen their offensive abilities to combat these threats. Governments that are open to public opinion are more likely to respond to perceived cyber security threats by using their competences and strengthening their capacity in cyber security capabilities, structures, and instruments.[23]

It is worth noting that the meaning of the term 'cyber security' is changing over time. Until recently, researchers focused mainly on technical risk management issues to protect critical information and infrastructure. Today, however, academics as well as policymakers view cyber threats as key challenges to national security.[24] In addition, the increasing digitization of many aspects of the economy, society, and politics raises cyber security concerns.[25]

There is a significant distinction in the literature between scholars conceptualising cyber security from a societal security perspective[26] and cyber threats in the context of state security.[27] There is a significant distinction in the literature between scholars conceptualizing cyber security from a societal security perspective and cyber threats in the context of state security. The first approach focuses on cyber security as activities concerning, among other things, law enforcement and technical solutions to protect the public during their daily use of digital services. From this perspective, cyber security policy is also concerned with the protection of digital rights, namely the right to privacy and freedom of expression online.

The second approach focuses on cyber threats and forms of violation of state sovereignty, which involves viewing cyber security as a military issue. This approach views cyber security as a national security issue and links it to a call for efforts

[22] R. Deibert and M. Crete-Nishihata, "Blurred boundaries: Probing the ethics of cyberspace research," *Review of Policy Research* 28 (2011): 531–537.

[23] M. Dunn Cavelty, "From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse," *International Studies Review* 15, no. 1 (2013): 105–122.

[24] *National cybersecurity and cyberdefense policy snapshots*, ed. R.S. Dewar (Zurich: Center for Security Studies (CSS), ETH Zurich, 2018).

[25] M. Dunn Cavelty and F.J. Egloff, "The politics of cybersecurity: Balancing different roles of the state," *St Antony's International Review* 15 (2019): 37–57.

[26] R. Deibert, "Trajectories of cyber security research," in *Oxford handbook of international security,* eds. A. Gheciu and W.C. Wohlforth (2017), 531–546; M. Dunn Cavelty, *Cyber-security and threat politics: US efforts to secure the information age* (London: Routledge, 2008); M. Mueller, *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace* (Cambridge, MA: Polity, 2017).

[27] Ch.C. Demchak and P. Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* (AL: Air Univ, Maxwell AFB, 2011); T. Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013); P.W. Singer and A. Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014).

to develop a transnational approach to cyber security. The transnational nature of internet infrastructure is combined here with the assertion of digital sovereignty.[28]

Technology has traditionally evolved faster than our ability to anticipate its impact on political, social, and economic systems. Consequently, attempts are being made to implement regulations, standards, and governance processes to control this impact, but these are often slower than technological developments. This is particularly evident in countries where the expansion of connectivity is developing much faster than the ability of the state, industry, and society to master and gain from the development of technical capabilities.[29]

State digital capability as a concept for cyber security

The process of digital transformation is currently a widely discussed and important topic in various sectors including business, governance, security, education, and industry, as all these sectors have undergone digital transformation. The EU created the Digital Economy and Society Index (DESI) in 2014 to assess the level of digitalization in member states and identify their main weaknesses. The index summarizes overall digital performance, tracks progress in digital competitiveness and productivity, and measures progress towards the digital economy and digital society. Cybersecurity is one of the essential components of the DESI index, as effective management of risks related to cyber threats and the protection of digital infrastructure are crucial for a developing digital economy and a technology-driven society. Therefore, the DESI index serves as a kind of indicator that points to the overall level of a country's readiness in terms of its digital society and economy, with cybersecurity being one of its significant elements. A high score in the cybersecurity area indicates that a given country is better prepared to deal with cyber threats, safeguarding individuals, businesses, and institutions from potential attacks.

This study uses key areas representing the main indicators of the index in the following areas of digitization: human capital, connectivity, digital inclusion, and digital public services. The results published by the European Commission in 2022 show that the Baltic States have made progress in the aforementioned areas since the first edition of the DESI index in 2014. Data from 2018 to 2022 was used for the analysis of the current state of digital development.[30] This study aims to comparatively elaborate the cyber security policy potential of the Baltic States, identify areas that need improvement, and propose a framework for future cooperation that can be expanded among Central European countries.

[28] Calderaro and Craig, "Transnational governance of cybersecurity: policy challenges," 917–938.

[29] C.A. Makridis and M. Smeets, "Determinants of Cyber Readiness," *Journal of Cyber Policy* 4, no. 1 (2019): 72–89.

[30] Developed based on own data, accessed June 2, 2022, https://digital-strategy.ec.europa.eu/pl/policies/desi.

In an overall analysis of the DESI results, it can be seen that Estonia has been at the forefront of the digital economy in the EU for years, which can be attributed to the government's early and strong investment in the technology sector (Table 1). Over the past five years, Estonia has performed very well in all categories, which is indicative of the country's high innovation and advanced cyber capacity building and development efforts. Although there were some exceptions, such as a lower score in the 'connectivity' category in 2022, these are not the norm. Estonia also made progress in the 'digital technology integration' category, with figures close to the EU average in the studied timeframe. Estonia continues to invest in digital development, digital education, and the development of innovative digital solutions for businesses and citizens in order to strengthen its digital leadership in Europe. In 2017, Estonia ranked 1st in the EU, with a score of 0.68, making it one of the leaders in the EU. In 2022, Estonia remains in 1st place, with a score of 0.79, which means that it is one of the leaders in the digital economy in the EU.

Lithuania has shown a significant increase in its score over the last five years, achieving higher results than the EU average, especially in the categories of 'digital technology integration' and 'digital public services'. It is worth noting that Lithuania has also performed well in the area of 'connectivity', with high scores except in 2022. However, in the category of 'human capital', the country has performed below average for a long time. Gradual improvement in this category is discernible through increasing digital skills of the population and adapting the education system to the requirements of a digital society. In 2022, the results in this category do not deviate significantly from the EU average, indicating that Lithuanian citizens have access to adequate training and tools to use new technologies. However, there is still room for improvement in this area, as digital skills in society have a positive impact on the development of the digital space in the country. Therefore, further efforts are needed to improve performance in this category. In 2017, Lithuania ranked 26th in the EU with a score of 0.43 (on a scale of 0 to 1), which was slightly below the EU average (0.52). In 2022, Lithuania moved up to 12th place in the EU, with a score of 0.63, which indicates that it has surpassed the EU average.

Latvia has also recorded an improvement in its DESI score but still remains below the EU average. However, the DESI score highlights the potential for further development of the digital economy in the Baltic States, which could contribute to the growth and competitiveness of their economies both in the EU and globally. Nonetheless, there are areas where Latvia could improve its performance, particularly in the 'human capital' category, which suggests a low level of digital-related skills and knowledge. This could lead to a lack of innovation in businesses, lower wages, and poorer working conditions for employees, as well as difficulties in accessing digital services for residents. Therefore, it is crucial for Latvia to increase its investment in training and digital competence development to improve the level of human capital and enhance the chances of developing a digital economy and society.

Table 1. Digital Economy and Society Index (DESI).[31]

	2018				2019				2020				2021				2022			
	Lithuania	**Latvia**	**Estonia**	**EU average**	**Lithuania**	**Latvia**	**Estonia**	**EU average**	**Lithuania**	**Latvia**	**Estonia**	**EU average**	**Lithuania**	**Latvia**	**Estonia**	**EU average**	**Lithuania**	**Latvia**	**Estonia**	**EU average**
1 Human capital	48,5	43,8	61,4	56,5	42,2	40,4	62,4	48,0	43,8	35,0	66,7	49,3	46,1	41,1	57,9	47,1	42,5	44,1	53,9	45,7
2 Connectivity	56,8	54,8	61,6	50,5	52,1	49,1	60,7	53,4	57,3	54,0	65,4	58,0	41,7	50,4	46,6	50,2	49,4	50,1	44,4	59,9
3 Digital technology integration	47,5	27,0	37,1	40,1	49,7	25,9	39,2	41,1	49,5	28,3	41,1	41,4	41,2	26,8	41,5	37,6	37,2	25,8	36,5	36,1
4 Digital public services	68,2	65,2	78,1	57,5	73,3	73,7	79,5	62,9	81,4	85,1	89,3	72,0	78,0	79,6	91,8	68,1	81,8	78,8	91,2	67,3

[31] Developed based on own data, https://digital-strategy.ec.europa.eu/pl/policies/desi.

In the category of 'connectivity', Latvia scored either above or close to the EU average over the period under review, indicating that the country has a well-developed network infrastructure. However, Latvia scored lower than the EU average in the category 'digital technology integration', which refers to the extent to which digital technologies are used in different sectors of the economy and society. A poor score in this category suggests that digital technologies are not fully utilized in Latvia's economy and society. In contrast, in the category 'digital public services', Latvia scored higher than the EU average, as did the other countries in the region, suggesting that public services are available online for citizens and can be easily accessed. This indicates that Latvia provides its citizens with easy and convenient access to public services, which has a positive impact on the quality of life and functioning of society. Nevertheless, Latvia still needs to improve its performance in 'human capital' and 'digital integration'. The challenge here is to continue to invest in innovation, particularly in the public sector, and in digital education so that the country's population has the necessary skills to benefit from the demands of the labour market and to use innovative digital solutions. In 2017, Latvia ranked 24th in the EU, with a score of 0.45, which was below the EU average. In 2022, Latvia moved up to 18th place in the EU, with a score of 0.57, which indicates an improvement in its score over the past five years, but still places it below the EU average.

The analysis of the DESI scores indicates differences in the development of the digital economy among the Baltic States, but it also shows that all three countries are making progress in this regard. Regardless of the performance differences, the Baltic States are generally well integrated with the internet, and their societies are increasingly using digital services, indicating a positive development trend.

However, there are challenges that may pose obstacles to the further development of the digital economies of the Baltic States. One of these challenges is the shortage of IT professionals, which is particularly acute in Estonia. In addition, Lithuania, Latvia, and Estonia have to compete with other EU countries and world leaders in digital technologies while dealing with data privacy and cybersecurity issues.

Despite these challenges, there are opportunities that can be leveraged, especially if the Baltic States continue to invest in the development of the technology sector and digital skills among their citizens. The growth of the digital economy can improve the competitiveness of the Baltic economies and accelerate the digital transformation process, which will have a positive impact on their position in the EU and internationally.

Elements for strengthening cyber security by the Baltic States

A turning point in the cyber security policy of the Baltic States was the Russian annexation of Crimea in 2014, which accelerated efforts to strengthen their political-military capabilities. Lithuania and Latvia have also increased their defence spending commitments with a goal to gradually reach 2% of GDP, following Estonia's example, which was one of the few NATO countries to maintain defence spending at 2% of GDP.[32] However, the main question now is the allocation of funds according to the '2% of GDP' principle.

Based on the latest information provided by the defence ministries of the respective countries, it is possible to characterize the expenditures related to raising the level of cyber security. In the case of the Baltic States, funding for cyber security comes from various sources, mainly the state budget. From 2017 to 2022, Lithuania, Latvia, and Estonia allocated significant amounts to cyber security. Estonia is the leader in this list, having allocated EUR 140 million over five years, followed by Lithuania with around EUR 54 million, and Latvia with EUR 16 million.[33]

The second important element of cybersecurity funding is European funds. Estonia allocated approximately EUR 30 million for cybersecurity in the 2014–2020 period, followed by Latvia with around EUR 16 million and Lithuania with more than EUR 14 million. In each of these three cases, the majority of the funds went towards developing the countries' cybersecurity capabilities, including strengthening network and system protection, developing skills and training for IT professionals, and funding government institutions and agencies responsible for cybersecurity. For the next European funding period, which runs from 2021 to 2027, each country plans to spend an additional EUR 10 million to EUR 16 million for this purpose.[34]

The third main source of funding for cyber security in the Baltic States is the private sector, which contributes to technology development through investment, as well as by working with government and public institutions to ensure data and infrastructure security. However, determining the scale of investment in this case is limited as many companies do not publicly disclose such information. Nevertheless, some examples of investments and actions taken by private companies towards improving cyber security in the region can be found.

There are several companies in the Baltic States that provide cyber security solutions and services, and many of them operate internationally. For example, in Estonia, Guardtime[35] offers solutions based on blockchain technology, and

[32] Bladaitė and Šešelgytė, "Building a Multiple 'Security Shelter' in the Baltic States," 1010–1032.

[33] Banka and Bussmann, "Uncomfortable neighbors: NATO, Russia," 1–24.

[34] Own calculations based on: *Report, European Cybersecurity Investment Platform,* 2022, accessed June 6, 2022, https://www.eib.org/attachments/lucalli/20220206-european-cybersecurity-investment-platform-en.pdf.

[35] *How the world's leading blockchain company Guardtime turns trust into digital truth from its Tallinn office*, accessed June 2, 2022, https://investinestonia.com/how-the-worlds-leading-blockchain-company-guardtime-turns-trust-into-digital-truth-from-its-tallinn-office/.

Veriff[36] deals with online identity verification. In 2018, Nortal,[37] a company that designs IT systems, among other things, announced an investment of EUR 2.5 million to develop its cyber security services.

There are also companies in Latvia that offer cyber security services and solutions, including Exigen Services,[38] which specialises in the design of IT security systems and critical infrastructure. In 2021, private banking company Citadele Banka announced that it will spend EUR 3 million to develop its cyber security capabilities.[39]

In the case of Lithuania, there are also examples of private companies investing in cyber security. NFQ Technologies announced that it has earmarked EUR 1.5 million to develop its IT security services,[40] and Devbridge announced that it has invested EUR 500,000 to develop its cyber security department.[41]

In addition to absolute boundaries set by factors such as defence GDP or investments in non-military cyber-security, it is worth analyzing the development efforts undertaken by states to build security capacity, particularly in the digital area. An example of this is the state budget expenditure on ICT (Information and Communication Technology), which illustrates the importance that a country's authorities attribute to the development and implementation of modern information and communication technologies. Such investments aim to streamline the functioning of public administration, improve business efficiency, and increase the accessibility of public services for citizens.

The relatively high spending on ICT may indicate the commitment of the authorities of all three countries to develop new technologies and improve the efficiency of their administrative systems (Table 2). This may also make the Baltic States more attractive as investment destinations for ICT companies. At the same time, appropriate investment in ICT infrastructure can help improve the quality of public services and increase internet accessibility for residents of the Baltic States.

[36] *Veriff raises $100 million and becomes Estonia's ninth unicorn*, accessed June 2, 2022, https://investinestonia.com/veriff-raises-100-million-and-becomes-estonian-ninth-unicorn/.

[37] *The American Dream of Nortal, the Company of the Year that built a third of e-Estonia*, accessed June 2, 2022, https://investinestonia.com/the-american-dream-of-nortal-the-company-of-the-year-that-built-a-third-of-e-estonia/.

[38] *Latvia – Your ICT Partner in Europe*, accessed June 2, 2022, http://petijumi.mk.gov.lv/sites/default/files/file/39%20-%20Latvia-your%20ICT%20partner%20in%20Europa.pdf.

[39] *EIB Group and AS Citadele banka announce a deal to support at least €460 million in new lending for Baltic businesses*, accessed June 2, 2022, https://www.eib.org/en/press/all/2022-512-as-citadele-banka-and-eib-group-announce-a-deal-to-support-at-least-eur460-million-in-new-lending-for-baltic-businesses.

[40] *NFQ Technologies brings valantic to Lithuania*, accessed June 2, 2022, https://investlithuania.com/news/nfq-technologies-brings-valantic-to-lithuania/.

[41] *Devbridge success story in Lithuania - Vilnius*, accessed June 2, 2022, https://investlithuania.com/success-stories/devbridge/.

It is noticeable that the high percentage share of the ICT sector in GDP, which ranged from 5.5 to 7.0 per cent in 2022, is increasing continuously. This indicates that these countries are viewing new technologies more as a condition for economic growth, which is also a condition for defence policy. Thus, the above data indicates how the Baltic States are building and developing their independent defence capabilities, which can be categorized as strengthening cyber capabilities. In conclusion, the Baltic States are successfully using the ICT sector as one of the tools to build their economies. Their higher share of GDP compared to the EU average suggests that they are able to compete in international technology markets, and their initiatives and investments in the ICT sector are at a good level (Table 3).

It is also worth noting that the Baltic States have increased their efforts in recent years to improve their research and development (R&D) activities, which is also contributing to building digital capabilities that can deter and discourage Russia from taking aggressive actions.

The Baltic States are increasing their spending on R&D compared to previous years. Investments in this area can have a positive impact on the development of

Table 2. Share of ICT sector in GDP.[42]

	2017	2018	2019	2020	2021	2022
Lithuania	3,03	3,13	3,49	3,8	5,3	5,5
Latvia	4,69	4,93	5,33	5,66	6,0	6,1
Estonia	5,12	5,39	5,95	6,79	6,9	7,0
EU average	4,33	4,45	4,59	4,63	4,89	5,23

Table 3. Gross domestic expenditure on research related to cybersecurity.[43]

	2017	2018	2019	2020	2021	2022
Lithuania	0,9	0,94	0,99	1,14	1,11	1,16
Latvia	0,51	0,64	0,64	0,69	0,69	0,74
Estonia	1,28	1,41	1,63	1,75	1,75	1,821
EU average	2,15	2,19	2,22	2,3	2,26	2,39

[42] *Eurostat, Database*, accessed June 2, 2022, https://ec.europa.eu/eurostat/data/database.

[43] *Eurostat,* https://ec.europa.eu/eurostat/data/database.

innovative solutions and the countries' economic competitiveness, which in the long term can benefit both the economy and society as a whole. Such investments aim to improve the countries' competitiveness through the development of new technologies, strengthen the entrepreneurial sector, and improve the quality of life of citizens through the development of new technological solutions. R&D expenditures therefore demonstrate the Baltic States' commitment to the development of new technologies and the pursuit of innovation and competitiveness in the international market. They can also contribute to the growth of employment in the science and technology sector, as well as to improving the living and working conditions of the region's residents through the development of new technological solutions.

Gross domestic spending on research and development in the Baltic States - Estonia, Latvia, and Lithuania - has been lower than the EU average over the past five years. However, these countries have increased their investment in R&D in recent years and have seen a growth in spending. It is worth noting that Estonia has achieved the highest level of R&D investment among the Baltic States. Meanwhile, Lithuania and Latvia have increased their spending in this area over the past few years and plan to continue investing in the future.

Based on their past achievements in the field of cybersecurity and investment in R&D, it can be assumed that all three Baltic states have great potential for patent filing in this area. Lithuania and Latvia are intensifying their cybersecurity efforts, increasing investment in R&D, and supporting the development of the IT sector.

The digital sector is an important part of Lithuania's economy. The country is actively promoting the development of innovative companies and startups through initiatives such as "Startup Lithuania".[44] In Latvia, the IT industry is one of the fastest- growing sectors of the economy, and there are initiatives to develop and promote innovation, such as "Riga TechGirls",[45] which encourage women to pursue careers in the technology industry.

However, Estonia is one of the leading countries in cyber security, well-known for its advanced digital infrastructure and innovative solutions in this field. In 2007, Estonia faced one of the first cases of a state-wide cyber offensive, which prompted the country to develop a digital strategy and strengthen its cyber security policy. Estonia has a number of initiatives, such as "e-Residency"[46] and "Data Embassy",[47] which aim to attract innovative digital businesses and protect critical data and

[44] *Startup Lithuania*, accessed June 6, 2022, https://www.startuplithuania.com/.

[45] *Riga TechGirls*, accessed June 6, 2022, https://rigatechgirls.com/.

[46] *e-Residency of Estonia*, accessed June 6, 2022, https://www.e-resident.gov.ee/.

[47] *Data Embassy*, accessed June 6, 2022, https://e-estonia.com/solutions/e-governance/data-embassy/.

services. Additionally, Estonia has numerous programs to support the development of startups and innovative digital businesses.

The thesis of the paper is based on the idea that the development of cyber capabilities depends on state resources to develop those capabilities, independent of political motivations. State initiatives are aimed at promoting cyber capabilities and are driven by both military paradigms and national access to scientific and technological knowledge and innovation. The motivation for building capacity in cyberspace can be driven by the desire to deter threats.[48]

Cyber threats, regardless of their impact, can create significant social pressure on those in power. Therefore, authorities are more likely to take steps to increase the professionalization of cyber capabilities in order to avoid negative costs. In other words, economic and political interests encourage authorities to increase their investment in cyberspace, partly due to the rise in cyber threats and fear of the costly consequences of harmful cyber activities.[49]

This analysis sheds light on the role played by the production of scientific and technological knowledge, interpreting cyber-security policy as a logic based on deterring the adversary.[50] For example, various programs and initiatives are introduced to increase innovation in the application of digital technologies.

For example, Lithuania has introduced the "Intellect LT+"[51] program, which aims to increase innovation in the economy by supporting investment in research and development, as well as the development of ICT competencies. Latvia, on the other hand, has launched the "Innovation Vouchers" program,[52] which aims to increase investment in research and development in small and medium-sized enterprises. Estonia, in turn, has an ambitious plan to increase R&D spending to 3% of GDP by 2027.[53]

In recent years, these countries have filed numerous patents in the field of cyber security, which is crucial to their cyber security policies. Patents allow the Baltic states to maintain a competitive edge in the field of cyber security, as they provide protection against other countries copying and exploiting their inventions.

[48] N.N. Schia, "The Cyber Frontier and Digital Pitfalls in the Global South," *Third World Quarterly* 39, no. 5 (2018): 821–837.

[49] S. Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," *Journal of Information Technology & Politics* 10, no. 1 (2013): 86–103.

[50] J.S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017): 44–71.

[51] *The Lithuanian road to Smart specialisation*, accessed June 8, 2022, https://projects2014-2020.interregeurope.eu/ecoris3/news/news-article/1611/the-lithuanian-road-to-smart-specialisation/.

[52] *Innovation Voucher program - Startup Latvia*, accessed June 8, 2022, https://startuplatvia.eu/innovation-voucher.

[53] *R&D expenditure increasing, on course for 3% of GDP in 2020*, accessed June 8, 2022, https://news.err.ee/882028/r-d-expenditure-increasing-on-course-for-3-of-gdp-in-2020.

The patents also allow the Baltic states to increase their security, as they can serve as tools to combat cyber threats such as hacking attacks and industrial espionage.

Compared to the EU average, the number of cybersecurity patents filed in the Baltic States is relatively low (Table 4). All three Baltic states have lower patent filing rates in this area than the EU average. However, it is worth noting that each of the Baltic states differs in terms of market size, number of innovative companies, and other factors affecting the number of patents filed.

While the data shows that the Baltic states have filed relatively few patents in the field of cybersecurity in the last five years compared to the EU average, it's important to note that the number of filings in this field does not necessarily reflect actual investment and technological development. There are other ways to protect inventions, such as business secrets or licensing agreements, which do not require patent filings. Moreover, in the context of cybersecurity and software development, much of the innovation may be protected by copyright rather than patents.

Filing patents in cybersecurity contributes to the image of the Baltic States as leaders in digital security. By investing in cybersecurity research and development, these countries gain a reputation as innovative and technologically advanced states.

Finally, cybersecurity patents can be a source of revenue for the Baltic States, as they can be sold or licensed to other countries and companies. This can help fund further investment in research and development, which in turn leads to even more progress in the field of cybersecurity.

Table 4. The total number of filed patents in the following areas: Computer technology, Telecommunications, Digital, Communications, Audio-visual technology, IT methods for management, Semiconductors.[54]

	2017	2018	2019	2020	2021	2022
Lithuania	29	27	27	27	21	18
Latvia	11	15	13	11	12	12
Estonia	37	47	42	38	39	36
EU average	3 205	3 764	4 142	4 498	4 539	4 636

[54] Data based on the European Patent Office, accessed June 8, 2022, https://new.epo.org/en/statistics-centre#/customchart.

Cybersecurity strategies as a direction for digital capacity development

In addition to building and shaping national capabilities, it is equally important to implement cybersecurity capacity-building strategies to enhance the country's potential as an active player in the international approach to cybersecurity management.

In this context, the promotion of relevant practices is addressed to specific stakeholders, including government and industry, as well as those representing civil society, to ensure the development of sustainable connections between these centres.[55]

In order to characterize the strategic documents that reflect the debate on cybersecurity, it is necessary to address key questions that shape public and academic discourse in the field of cybersecurity in the Baltic States. These questions include: What factors determine the existing capabilities of the state in cybersecurity? What assumptions have been made in the documents so far that allow us to understand the process in the context of building the state's capabilities in a regional and global sense? What aspects do the authors of the strategies prioritize for the development of cybersecurity capabilities?

Cybersecurity strategies are part of national security and are becoming increasingly important due to the pervasive impact of cyber technology.[56] In this section of the work, a strategic document analysis was conducted to identify key passages that illustrate the development of digital capabilities as a critical element in building cybersecurity. The strategic documents analyzed were those focusing on cybersecurity in the Baltic States, including the *National Cyber Security Strategy of Lithuania* [Lithuania 2018], the *Cyber Security Strategy of Latvia 2019–2022* [Latvia 2019–2022], and the *Cybersecurity Strategy Republic of Estonia 2019–2022* [Estonia 2019–2022].

Since the scope of the analysis of the cyber security strategy focuses on improving the efficiency of countries in the use of digital technologies, four categories of data from the Digital Economy and Society Index (DESI) were used to assess the level of development (maturity) of cyber security policies. According to this yardstick, in 2022, Estonia is the leader, Latvia ranks 8th, and Lithuania 15th in the European Union.

All three countries recognize the close connection between cybersecurity and the economic sector, and are aware that harmful digital activities targeting critical infrastructure can destabilize public services. With a focus on human capital, the Baltic states are prioritizing their cyber security strategies on educating the public and developing a cadre of cyber security professionals. Each country

[55] B. Valeriano, B. Jensen and R.C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford: Oxford University Press, 2018).

[56] Bailes, "Does a Small State," Occasional Paper, 2009.

has various programs and initiatives aimed at increasing public awareness and knowledge of cybersecurity, as well as preparing professionals to work in the cyber security sector. Estonia places a strong emphasis on educating the public about cyber security.

"As part of the Lifelong Learning Strategy 2014–2020, 45 efforts are being made to ensure that competences pertaining to digital skills also include cybersecurity, and that besides digital technology, elementary knowledge related to cybersecurity are also integrated into curricula. The objective of the lifelong learning strategy's digital revolution programme is the smart and knowledge-driven integration of digital opportunities into the academic process and thereby ensuring the development of digital competence including competences related to security In the field of general education". [Estonia 2019–2022, 31].

Latvia's strategy also emphasizes the importance of providing training and seminars for various groups, including entrepreneurs and public sector employees.

"The education system in Latvia is oriented towards creating an information society. This is a society that knows how, can and has the capacity to acquire information using ICT, combine it with existing knowledge and use the newly acquired knowledge for its own benefit. At the same time, efforts should be made to increase the general knowledge of the public for the education and development of young IT professionals, where opportunities to participate in thematic educational events and competitions in the field of cyber security are Essentials." [Latvia 2019–2022, 18]

The above points are also articulated in Lithuania's cyber security strategy, which places emphasis on the development of a pool of cyber security experts.

"High-quality public education that meets the needs of the labour market is a tool that can contribute to the Professional labour market is a tool that can contribute to professional competence. [...] In order to reduce the gap between supply and demand for cyber security professionals, there should be existing cybersecurity study programmes need to be improve existing cyber security degree programmes and establish new degree programmes." [Lithuania 2018, 13]

Each of these countries is investing in the development of 5G networks and digital technologies to enhance the security of their national communication infrastructure. However, Estonia is particularly focusing on the development of digital technologies and communication infrastructure due to an urgent need for corrective action in this area.

"The spacious autonomy when it comes to development and administration of IT systems results in a situation where institutions organize administration of cybersecurity risks often without appraising the broader impact of their decisions, even though they are connected to the public infrastructure (state network). Disregard for or the absence of common security principles and standards jeopardizes the functioning of Estonia's digital services, which are based on dispersed architecture.

The state still lacks a systematic view of the mutual cross- and cross-border dependencies and potential impacts of systems and a clear view of ensuring the minimum level of services that should also be operational in a crisis." [Estonia 2019–2022, 26].

The tasks mentioned above are articulated similarly in the Latvian strategy. Along with investments in the development of communication infrastructure and digital technologies, the strategy emphasizes the modernization of the broadband network and the development of 5G networks as crucial elements of cyber security.

"The latest generation of ICT solutions offers the possibility to quickly and conveniently obtain comprehensive information about events and processes in Latvia or abroad at any time and place, communicate and exchange information, make transactions and payments online, receive electronic services, create, sign and send electronic documents and save information electronically, using the advantages of smart devices and cloud computing providers on a daily basis." [Latvia 2019–2022, 5]

Lithuania is also focusing on developing digital communication infrastructure and building robust security mechanisms for telecommunication networks with the participation of the private sector.

"In modern states, in which the broadband infrastructures are well developed, public sector representatives as well as managers of critical information infrastructures who are often private sector representatives, are not always able to combat cyber incidents independently. Thus cooperation between public and private sectors becomes inevitable in order to ensure comprehensive cybersecurity. The PPP success factor is a fully-fledged partnership, which entails trust and mutual benefit. Thus public and private sectors should strive to work together to this end." [Lithuania 2018, 16]

Each of these countries is investing in projects that focus on developing digital platforms and implementing technologies such as blockchain, IoT, or smart city solutions. These efforts aim to improve the efficiency and quality of public services, as well as enhance the security of digital infrastructure. The Estonian document emphasizes the importance of electronic platforms, which facilitate contact between citizens and the state administration, with the goal of:

"Administration of the complexity of projects and minimization of red tape for the state, private sector through both legal and public administration measures." [Estonia 2019–2022, 18].

Latvia also recognizes the importance of integrating digital technology, with the aim of, among other things, facilitating access to health and legal services through digital platforms.

"The aforementioned indicators point to the formation of a digital society in Latvia, where the use of ICT solutions and digital technologies underpins prosperity, economic activity and growth. […] National cyber-security governance is based on mutual cooperation, where in the performance of each state institution's functions, including in cyberspace, there is direct cooperation with other institutions and the private sector or cooperation in the National Information Technology Security Board." [Latvia 2019–2022, 8]

Like other countries, Lithuania is also focusing on measures to enable citizens to access government services through digital platforms.

"With regard to rapid development of cyberspace, various opportunities for innovation, which, in turn, drives economic and productivity growth, have emerged. This prompts the creation of new and better jobs, increases social mobility and responds to social and security challenges globally. [...] In modern states, in which the broadband infrastructures are well developed, public sector representatives as well as managers of critical information infrastructures who are often private sector representatives, are not always able to combat cyber incidents independently. Thus cooperation between public and private sectors becomes inevitable in order to ensure comprehensive cybersecurity. The PPP success factor is a fully-fledged partnership, which entails trust and mutual benefit. Thus public and private sectors should strive to work together to this end." [Lithuania 2018, 16]

The Baltic States have long emphasized the development of digital public services. In their cybersecurity strategies, these countries aim to ensure the security of digital public services available to citizens, businesses, and public administration. As part of its cybersecurity strategy, Estonia is focusing on ensuring the security of digital public services through the use of solutions such as cryptography, authentication, and identity verification.

"It is critical important for the state to ensure secure and functioning Communications and data exchange between systems meant for various areas of administration and authorities (including telephone communication and internet connection). To do this, it is planned to develop for the first time a comprehensive vision – a state communication concept that will map out the need for Communications on in both ordinary and crisis situations. Based on this, it will be possible to map development needs, plan activities and put in place the division of tasks and how they are organized between different parties. Further, it is planned to continua expanding and developing the state data communication network and the transition to encrypted e-correspondence and data communication for ensuring secure communication between government institutions." [Estonia 2019–2022, 43].

The Latvian document highlights the significant facilitation provided by digital technology in areas such as e-taxes, e-registration of companies, and e-healthcare services. However, it also emphasizes the importance of ensuring the security of digital public services, which require respect for privacy and protection of personal data.

"Latvia's cyberspace continues to be exposed to large-scale threats - phishing campaigns, ransomware and malware, attempts to hack into systems, networks and websites, attacks to deny access to critical IT systems, and fraudulent email and social engineering campaigns to obtain personal data or credentials to discredit a specific person, company or institution or to commit a crime. […] Given the dangers inherent in the wider use of ICT, there is a need to increasingly mitigate potential risks. It is necessary to strike a balance between effective governance and the right to privacy in cyberspace so as not to hamper innovation, development and efficiency." [Latvia 2019–2022, 11]

Lithuania also views the development of digital public services as crucial, identifying it as the foundation for building an effective state defence in cyberspace.

"However, all efforts of the state in this direction must be focused on support measures that promote international networking in finding potential employees and partners. This would stimulate private sector investment in the R&D and innovation areas, new technologies, tools and services and in the cyber security area as well. The designing of innovative cyber security products would not only provide additional support and leverage for the competitiveness of the Lithuanian industry, but it is a key factor in responding to modern cyber incidents." [Lithuania 2018, 13]

A review of national cybersecurity strategies in the three Baltic States reveals that cyber security strategies in the region are becoming more integrated and comprehensive. The strategies approach cyber security in a holistic manner and encompass economic, social, legal, technological innovation, and military aspects of cyber security. An analysis of the documents shows great similarities in perceptions of the challenges in developing cyber capabilities among the Baltic States, which emphasize the importance of digital public services in increasing state efficiency and improving contact with citizens. Targets related to developing and improving the quality of available digital public services, including e-health and e-education, appear in each strategy. Lithuania, Latvia, and Estonia strongly emphasize the need to ensure digital security in public services, including by increasing user knowledge and awareness and developing protection tools and systems.

Differences in the area of goal formulation in cyber security strategies between these countries are small. For example, Estonia's strategy focuses on ensuring the availability of digital public services through the development of technological infrastructure, such as high-speed Internet and 5G networks. Lithuania is turning its attention to developing digital tools and applications that will improve the use of public services and ensuring digital security for online transactions. Latvia is focusing on providing broad access to public services to equalize socioeconomic opportunities for different social groups, paying particular attention to the elderly and those with disabilities.

There is no significant difference between the Baltic States in the perception of the development of digital potentials, and the distribution and emphasis of certain accents is natural - as can be seen in the case of other countries in the region, which is more due to the political culture that each country has. In addition, the Baltic States are part of the EU and obliged to comply with the standards and rules set by the EU on cyber security. In the EU's latest cyber security strategy, the EU Cyber Security Strategy 2021–2025, the European Union aims to increase the EU's resilience to cyber threats, promote a culture of cyber security, strengthen international cooperation on cyber security, and accelerate the development of European cyber diplomacy.

Their cyber security strategies also focus on increasing resilience to cyber threats. Therefore, it's worth remembering that the goals of all three strategies are aligned - they aim to make the use of public services efficient, effective, and safe through the use of new technologies and digital tools.

Conclusions

This thesis discusses the significance of cybersecurity for the Baltic States, which perceive Russia's increasing power and new technologies as threats to their national security. The Baltic States are prioritizing the development of their defence and deterrence capabilities, and cybersecurity has become a key element of this strategy. Due to limited military capabilities and resources, the Baltic states are increasingly leaning towards considering the development of digital potential as an important means of strengthening their defence capabilities. To ensure a sufficient level of cybersecurity, the states must implement appropriate measures such as investing in research and development, aligning resources of different areas of the state and its institutions, and developing and implementing measures in line with strategic documents at national and international levels.

The thesis indicates that the development of digital capabilities is vital to strengthening the defence capabilities of the Baltic States. Therefore, the Baltic States must continue to invest in research and development, align resources of different areas of the state and its institutions, and develop and implement strategies in line with strategic documents at national and international levels. This way, the Baltic States will be able to effectively secure their systems against cyber threats, which is crucial for their defence capabilities in the region.

As technology advances, cybersecurity threats are likely to increase. Therefore, it is crucial for states and international communities to work together to prevent these threats and protect the interests of their citizens. Areas such as cryptography, artificial intelligence, machine learning, and the internet of things are becoming increasingly important. While the introduction of new technologies increases the efficiency of the state and private sector, it also creates new vulnerabilities in information systems that can be exploited by cyber criminals and states for espionage purposes or to destabilize the situation in a country.

In the context of the Baltic States, the increased risk of cyber threats is particularly important, given the geopolitical circumstances of the region and tensions in relations with Russia. Lithuania, Latvia, and Estonia are aware of the threats posed by Russia's cyber activities and are taking effective steps to enhance their defence capabilities. The Baltic States are actively implementing strategies and tools to detect and counter cyber-attacks and conducting educational campaigns to raise public awareness of cybersecurity risks.

In conclusion, developing digital capabilities and securing against cyber threats are key challenges for the Baltic States and other countries around the world. Security in cyberspace is becoming increasingly important, as many areas of life and the economy already operate solely on the basis of information systems. Therefore, states should actively work to strengthen their defence capabilities and prepare themselves to counter a cyber-attack to ensure the security of their citizens and business entities.

Data availability

All data underlying the results are available as part of the article and no additional source data are required.