CYBERSECURITY POLICY ANALYSIS AND RESEARCH COOPERATION IN THE BALTIC STATES

***Sandra Vasilevska [1], Edgars Vasilevskis[2], Zane Vitolina[1]**
[1]Latvia University of Life Sciences and Technologies, Latvia
[2]Riga Stradins University, Latvia
*Corresponding author's email: sandra.vasilevsky@gmail.com

Abstract
In the digital era, cybersecurity has emerged as a cornerstone of national security and economic resilience, especially for the geopolitically sensitive Baltic States - Latvia, Lithuania, and Estonia. This study examines the evolution of cybersecurity policy and research collaboration in the region, highlighting significant disparities in research output, institutional capacity, and policy development. Using a mixed-methods approach that combines bibliometric analysis from Scopus (2012–2024) and qualitative review of national and EU-level cybersecurity strategies, the research evaluates the alignment between policy frameworks and research efforts. The findings reveal Estonia as the regional leader in cybersecurity research, accounting for 54% of publications, driven by early investments and the presence of NATO's Cooperative Cyber Defence Centre of Excellence. Conversely, Latvia and Lithuania show slower progress, hindered by delayed strategic planning and overreliance on EU funding. In addition, statistical analysis in ANOVA was applied to assess the relationship between funding and the increase in publications. Furthermore, while research collaboration across the region exists, it remains fragmented and underutilised. The paper proposes cooperative models between key institutions and emphasises the need for a unified regional cybersecurity research strategy. Multidisciplinary integration and increased national investment are critical to advancing cyber resilience. Strengthening intra-regional collaboration and diversifying funding mechanisms is imperative to enhancing the Baltic States' cybersecurity posture and contributing to the EU's collective digital defence.
Keywords: cybersecurity policy, cyber threat intelligence, cyber resilience, research collaboration.

Introduction

Cybersecurity has become the foundation of national security and economic stability in the digital age. In recent years, the Baltic States – Latvia, Lithuania and Estonia – have faced increasing cyber threats targeting critical infrastructure, government institutions and the private sector.

Some of the most intense cyberattacks targeting Latvia occurred on November 14 and November 22, 2022. During these incidents, the hacktivist group Killnet used Telegram to disseminate calls for coordinated distributed denial-of-service (DDoS) attacks against various institutions across the Baltic region. The targets included entities within the national security and defence sectors (CERT-LV, 2023). In addition to geopolitical challenges, the regulatory environment of the European Union (EU) is becoming increasingly rigid. The NIS2 Directive, which entered into force in 2023, requires countries to strengthen cybersecurity requirements by introducing stricter frameworks for companies and public authorities.

At the same time, cooperation between the Baltic States in research and cybersecurity has developed significantly, especially in the context of integration and regional initiatives of the European Union. The EU Strategy for the Baltic Sea Region, established in 2009, has been an important tool for fostering cooperation in various policy areas, including cybersecurity and research (Szejgiec-Kolenda & Duma, 2020). This strategy has significantly strengthened the cross-border cooperation of the Baltic States, which is necessary to address cybersecurity challenges more effectively.

The importance of cybersecurity policy is also shaped by increasing social, economic, and technological pressures from governments. Countries are increasingly trying to develop their cybersecurity capacity to remain competitive internationally and protect critical infrastructure (Deibert & Crete-Nishihata, 2011). This trend proves that cybersecurity policy is no longer just a technical framework – it is a key factor in the strategic development of countries.

These threats, regulatory requirements and regional cooperation initiatives show that cybersecurity policy is no longer just a technical issue but a critical political and economic priority.

The Baltic States have actively developed their cybersecurity strategies. However, their policy coordination and cooperation in research are still fragmented. The main problems hindering an effective regional cybersecurity policy are insufficient regional cooperation – although all three Baltic States are EU and NATO member states, their cybersecurity research and policy development is mainly carried out separately rather than coordinated and the allocation of funding and resources – research and innovation in cybersecurity mainly depend on support from EU funds, which may not be stable enough in the long term.

This study aims to analyse the dynamics and structure of the results of cybersecurity research in the Baltic States in the framework of cybersecurity policy development. The analysis of the international research partnership in Latvia, Lithuania, and Estonia can provide insight into the research potential of the Baltic States in the field of cybersecurity and the potential for building mutual assistance mechanisms.

The geopolitical situation, digitalisation, changes in the international security environment, military aggression and cyberattacks, threats to national security in recent years have facilitated both research and the establishment of new laws, regulations and

policies to develop priority directions and an action plan for the prevention of threats to national security. In the European Union, the Baltic States, which include Latvia, Lithuania and Estonia, play a special role in cybersecurity. These countries, which are at the crossroads of geopolitical tensions, have become focal points for cybersecurity discussions due to their strategic location, technological progress, and historical experience with cyber threats. The collaboration among the Baltic States in research and cybersecurity has evolved significantly, particularly in the context of European Union (EU) integration and regional initiatives. The EU Strategy for the Baltic Sea Region, established in 2009, has played a pivotal role in fostering cooperation among these nations. This strategy has addressed various policy domains, enhancing transborder collaboration among the Baltic States. Consequently, understanding Latvia, Lithuania, and Estonia's cybersecurity policies is extremely important to understand the wider European cybersecurity environment and identify areas for collaborative research initiatives and improvement of decision-making systems.

There is insufficient strategic and sustainable coordination and cooperation between industries, cybersecurity research communities and governments. The Union suffers from insufficient investment and limited access to know-how, skills and equipment in the field of cybersecurity, and only a few of the Union's cybersecurity research and innovation results are translated into tradable solutions or scaled up across the economy. Cybersecurity has become a critical area of security challenges in today's interconnected world, and the increasing frequency and complexity of cyber threats underline its importance. As countries seek to protect their digital infrastructure and data assets, policymakers are tasked with formulating robust cybersecurity policies to mitigate risks and ensure cyberattack resilience. One of the regions at the forefront of these efforts is the European Union (EU), where Member States have recognised the need for collective action to address cybersecurity challenges effectively. The new Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022, also known as the NIS2 Directive (Directive (EU) 2022/2555), has entered into force, providing for the implementation of measures to achieve the same high level of cybersecurity in all EU Member States (European Union, 2022). In all three Baltic States, significant steps are being taken to implement the NIS2 Directive, focusing on legislative changes, compliance of companies and international cooperation.

Article 7 requires Member States to adopt, as part of their national cybersecurity strategies, policies to promote and develop R&D initiatives and to support academic and research institutions in the development of cybersecurity tools. The list of critical sectors also includes research organisations. In Latvia, cabinet regulation No. 158, adopted on 28 March 2023, 'On the Cybersecurity Strategy of Latvia for 2023-2026' (Latvian Cabinet of Ministers, 2023), also stipulates that the courses of action are public awareness, education and research and action direction for 'International cooperation and justice in cyberspace'. To understand the following policy steps and opportunities for cooperation, it is necessary to identify the current state of research and collaboration in the field of co-security.

The cybersecurity policy of the Baltic States reflects a multifaceted approach, which includes the legal framework, institutional mechanisms and international partnerships aimed at improving cyber resilience and protecting national interests. Given their relatively small size and common historical heritage, these countries often work closely within the EU framework to address common cybersecurity challenges while adapting strategies to their specific context.

The main research objects of our research are the cybersecurity policy and research cooperation of Latvia, Lithuania and Estonia, the legal framework, the chronology of cybersecurity laws adopted by each country and their analysis, including rules related to data protection, incident response and critical infrastructure protection. Understanding the regulatory framework is essential to assess the scope of cybersecurity governance and identify areas where harmonisation or improvement is needed.

In cybersecurity, the Baltic States have recognised the importance of collective action to enhance their cybersecurity posture. Research indicates that while there is a tendency for collaboration outside the Nordic-Baltic region, the need for a unified approach within the region is increasingly acknowledged (Sandnes, 2021).

By delving into these research objects, insights can be gained for research cooperation in the Baltic States; this study seeks to promote knowledge sharing, capacity building and innovation in cybersecurity management, thus improving the collective resilience of the European Union and its Member States against cyber threats.

The novelty of the research is that it is an interdisciplinary approach that analyses and integrates security research trends and technological development with potential research cooperation networks of the Baltic States and appropriate policies in the security field. This can help identify and develop new technologies and approaches to address security challenges.

The central aspect of the novelty of the study is the mapping of cybersecurity cooperation models of the Baltic States, which has not yet been thoroughly analysed in the research literature. Also, the integration of technological development and research trends with security policy creates a holistic view of regional cybersecurity and the development of practical recommendations for cybersecurity research networks in the Baltics, which could contribute to developing and implementing new security solutions in the policy.

Materials and Methods

This study used a tiered methodology that combined bibliometric analysis and qualitative policy document analysis. The integration of these methods made it possible to identify the main challenges and development trends and develop recommendations for more effective regional cooperation in cybersecurity. While several studies explore European cybersecurity trends, few focus on the Baltic states as a distinct geopolitical and scientific unit. The integration of regional strategy documents, national research outputs, and funding structures across Latvia, Lithuania, and Estonia has not been comprehensively addressed in existing literature. The combination of methods provided a full-fledged analysis, combining empirical data on research development and the evaluation of regulatory policy. The design of the study was based on bibliometric analysis to identify research activity in the field of cybersecurity in the Baltics, qualitative content analysis of documents, analysis of policy documents and strategies to identify Baltic cybersecurity research cooperation networks.

To study the dynamics of cybersecurity research, the Scopus database (Elsevier, n.d.) was used, where the analysis of publications was carried out, searching for information by the keywords formula, 'cybersecurity', or 'cyber security', or 'information security', 'Baltic States', or 'Latvia', or 'Lithuania', or 'Estonia'. As a parameter, the period from 2012 to 2024 was used. The data selection was carried out using the Boolean search method, which allows you to accurately formulate search terms and expand or narrow the results, depending on the keywords chosen.

Analysed documents: Latvian Cybersecurity Strategy 2023-2026 (Latvian Cabinet of Ministers, 2023), Lithuanian National Cyber Security Strategy 2022 (Ministry of National Defence of Lithuania, 2022), Estonia's National Cybersecurity and Cyberdefense Posture (Center for Security Studies, 2020), EU NIS2 Directive Implementation Guidelines (Directive (EU) 2022/2555) (European Union, 2022). All cybersecurity policy documents analysed in this study were available in English as official translations or published versions provided by national ministries or cybersecurity agencies. A manual thematic analysis was also carried out to identify key cybersecurity policy priorities.

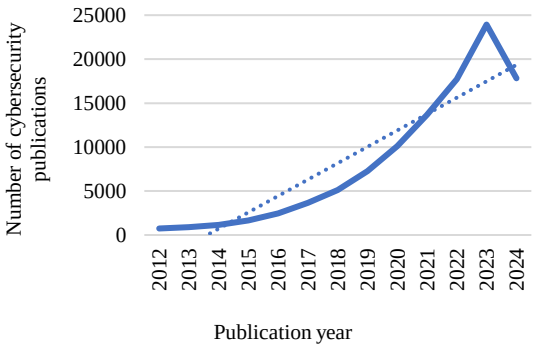
The statistical ANOVA analysis used the dependent variable - the number of cybersecurity research publications. This represents the total number of cybersecurity-related research papers published between 2012 and 2024 in Estonia, Latvia, and Lithuania. The data were obtained from the Scopus database (Elsevier, n.d.) by filtering for publications affiliated with institutions in these three countries. The Independent variable (categorical) is the country (Estonia, Latvia, Lithuania). The three Baltic States serve as categorical factors to assess whether there is a statistically significant difference in the number of publications among them. The primary objective of ANOVA and correlation analyses was to determine whether differences in research output among the Baltic States were statistically significant and whether those differences could be explained by variations in funding levels.

Results and Discussion

Concerning cybersecurity research, which can be found in the Scopus database (Elsevier, n.d.) under the keyword 'cybersecurity' in the period 2012-2024, the total number of publications found is 106256 documents; the graph of the trend of growth in publications is shown in Figure 1, which confirms that cybersecurity is a particularly relevant topic of security research around the world. However, it is new, dated to the first documents in 2000, and has a notable increase with each passing year, starting in 2016. The apparent drop in 2024 is likely due to incomplete indexing in the Scopus database at the time of data extraction (March 2025). Publications from late 2024 may not have been fully processed or included yet.

Figure 1

Growth in cybersecurity research publications (2012-2024)



Source: Scopus.

Cybersecurity research in the Baltic States has developed rapidly, especially after 2016, when European Union (EU) cybersecurity frameworks and funding programmes were introduced. Bibliometric data from Scopus (Elsevier, n.d.) show that between 2012 and 2024, Baltic scientists published 756 scientific articles in cybersecurity. Latvian scientists have published 128 (17%) documents, Lithuanian scientists 220 (29%) documents, and Estonian scientists 408 (54%) documents, becoming the leaders of the Baltic States in the field of cybersecurity research publications. This could be due to the historic trigger point on 27 April 2007, when Estonia experienced a series of politically motivated cyberattacks that lasted for 22 days. (Estonia's National Cybersecurity and Cyberdefense Posture, 2020) Moreover, the presence of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn and the government's early investment in cybersecurity research following the 2007 cyberattacks. The dominance of Estonia in publication

output is not merely quantitative but reflects deeper institutional readiness and strategic alignment. Estonia's early policy adoption and embedded cyber defense infrastructure (e.g., CCDCOE) correlate strongly with publication volume and collaboration intensity.

This fact also contributed to the creation of Estonia's first cybersecurity strategy in 2008, which is regularly being improved. In 2008, Estonia's cybersecurity strategy aimed to intensify research and development in cybersecurity and promote international cooperation in research. The example of Estonia shows that research in this area existed before the problem; the problem gave rise to policy, and research followed it with a 15 per cent increase in research articles after 2007. Latvia developed its first Cybersecurity Strategy 6 years later, in 2014, but Lithuania's first cybersecurity strategy was developed and approved in 2011. It must be concluded that in the case of Lithuania and Latvia, scientific research in cybersecurity was much more proactive regarding time than policymaking.

By analysing the data using statistical methods, the ANOVA test ($p = 0.0137$, $F = 4.84$) confirms statistically significant differences in the number of publications between Estonia, Lithuania, and Latvia. Tukey's post-hoc analysis of the HSD shows that Estonia is statistically significantly ahead of Latvia and Lithuania, which indicates a stable and long-term growth in scientific activity. This difference is due to the presence of the NATO CCDCOE Centre in Tallinn (CCDCOE, n.d.), the early implementation of the cybersecurity strategy (2008) and the high rating of the Global Cybersecurity Index (GCI) (88.5).

Lithuania and Latvia, on the other hand, are lagging significantly behind, as the first cybersecurity strategies were adopted later (Latvia – 2014, Lithuania – 2011), and the national funding of these countries for cybersecurity research is still limited. The Tukey test did not identify significant differences between Lithuania and Latvia, which shows that the dynamics of cybersecurity research in both countries are similar. The results of ANOVA and post-hoc analysis confirm significant differences in cybersecurity research activity in the Baltic States, and Estonia is the regional leader in terms of the number of publications and the level of research infrastructure and international cooperation.

Analysing the number of scientific publications in cybersecurity among the universities of the Baltic States, it can be concluded that Estonian institutions dominate this area. Out of a total of 1234 scientific documents, Tallinn University of Technology (TalTech) and Tartu University account for the largest share of publications, while in Lithuania, the most significant contributions are provided by Kaunas University of Technology and Vilnius Gediminas Technical University, and in Latvia by Riga Technical University.

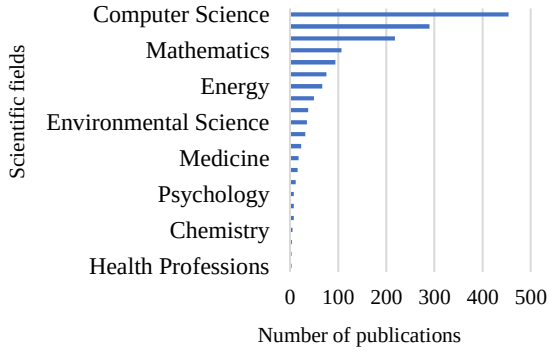
Of all the publications analysed, 45% are peer-reviewed journals, followed by conference proceedings with 42.6%, while book chapters and scientific reviews account for 7.8%. The proportion of conference papers indicates active involvement in international cybersecurity and technological development. The high proportion of conference materials indicates strong international cooperation, as the cybersecurity industry is developing rapidly, and the latest research is presented at international conferences before being published in journals.

Estonia's cybersecurity research leadership is closely linked to the widespread cyberattacks in 2007, catalysing the development of a national cybersecurity strategy and international cooperation. Following these events, the NATO Centre of Excellence for Cooperative Cybersecurity (CCDCOE) was established in Tallinn, which has played a key role in the development of research and international projects (CCDCOE, 2020), the Estonian Defence Forces Cyber Training Centre since 2012 and the Estonian Centre for Digital Development since 2017, promote cooperation with global experts and also funding for research. Although Latvia developed the Cybersecurity Strategy in 2014, its impact on scientific research became noticeable only after 2018, when the attraction of EU funds for research increased. Meanwhile, the establishment of the Lithuanian National Cyber Security Centre in 2023 is just beginning to have an impact and additional data are needed to assess its long-term research effectiveness. The Lithuanian Cybersecurity Strategy was established in 2011, and the first cybersecurity law was adopted in 2018.

Computer science and engineering dominate when analysing the scientific fields in the Baltic States, where cybersecurity-related publications have been produced. However, social sciences, mathematics, decision-making science, business and management, and energy also play a significant role, as illustrated in Figure 2.

Figure 2

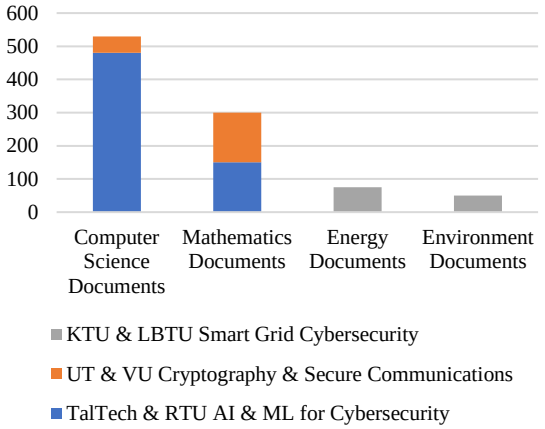
Research Publications by Field in Cybersecurity in Scopus (2012-2024)



These findings suggest that effective cybersecurity requires a multidisciplinary approach, integrating technical, social, psychological, and legal dimensions. Cooperation between universities in the Baltic States can significantly improve the quality and scope of cybersecurity research. By joining forces and

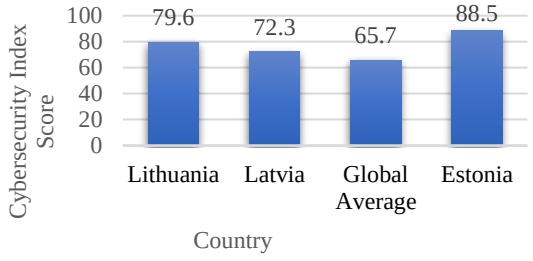
specialisations, universities can achieve better results and significantly contribute to ensuring cybersecurity. By analysing the research directions of universities in the Baltic States in the field of cybersecurity, potential opportunities for cooperation can be identified to use resources more efficiently and expand the scope of research. Potential cooperation models Figure 3 have been created based on the analysis of previous data.

Figure 3
University collaboration (2012-2024) in cybersecurity research (Baltic States)



Particularly successful collaboration partnership models could be established between TalTech (Estonia) and RTU (Latvia): Collaborative projects on AI and machine learning for cybersecurity, focusing on threat detection and incident response.
UT (Estonia) and VU (Lithuania): Joint research on cryptography and mathematical models for secure communications and data storage. KTU (Lithuania) and LBTU (Latvia): Collaborative research on smart grid cybersecurity, aiming to develop security solutions for energy distribution.
This study provides valuable insights into the development and challenges of cybersecurity research in the Baltic States. The results can serve as a basis for further collaborative research and policymaking to ensure a safer and more resilient cyberspace.
No matter the desire and necessity for research cooperation and policymaking in cybersecurity in the Baltic States, practical collaboration in cybersecurity research is closely related to the available funding.
By aligning research priorities with policy objectives, the Baltic States can use their strengths in the field of cybersecurity to build a more resilient society and economy. The Global Cybersecurity Index (GCI) (International Telecommunication Union, 2024) serves as a windstorm for the impact of research funding and policy-making in the Baltic States. The GCI objectively measures national commitments to cybersecurity, covering key pillars (legal, technical, organisational, capacity building and cooperation measures). For politicians, this index serves as a report highlighting strengths and weaknesses, guiding strategic planning, resource allocation, and the need for investment. Higher GCI scores may make it easier to justify further or increased investment in cybersecurity research and infrastructure. Strong performance signals the effectiveness of current strategies, while countries with lower GCI scores may need to step up efforts and investment. Estonia, with 88.5 and a leading top 10 GCI score - Figure 4, can be associated with strategic early investments in digital infrastructure and cybersecurity. The emphasis on cybersecurity since the 2007 cyberattacks has contributed to strong research results and effective policies.
The Lithuanian indicator 79.6 reflects a balanced approach to different pillars of cybersecurity. Its efforts to establish a national cybersecurity hub and implement a coherent regulatory framework have made a positive contribution. Latvia's 72.3 indicator indicates progress and growth opportunities. Targeted investments in capability development and cybersecurity programs can help improve its GCI rating. Closer cooperation between research institutions and government agencies could improve the impact of cybersecurity policies.
Considering the dominance of computer science and mathematics in cybersecurity research, the Baltic States should prioritise funding for projects that translate these theoretical achievements into practical applications. Figure 3 confirms that computer science is the main branch of science (over 450 documents), but mathematics also occupies an important place. Research on the security of smart electricity grids is significant for Estonia, Lithuania and Latvia. The energy sector is the third most important field of research in cybersecurity (50-100 documents). Social sciences and psychological studies that can help understand human behaviour and motivation in cyberattacks are also important in cybersecurity. Many other branches of science, such as chemistry, health professions, and medicine, also play a significant role (0-50 documents).

Figure 4
Cybersecurity Index Scores in 2024



Source: Adapted by author from International Telecommunication Union (2024).

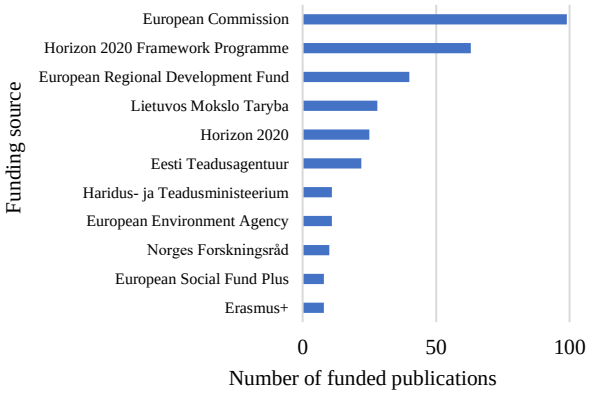
The Cybersecurity Index of the Baltic States (International Telecommunication Union, 2024),

Figure 4, is above the global cybersecurity index, which shows more outstanding commitment and efficiency in cybersecurity compared to the global average and shows that the Baltic States have made significant investments in cybersecurity. The most important sources of finance for cybersecurity research are funding from the European Union and the European Commission for research projects, mainly Horizon 2020 and the European Regional Development Fund. This is evidenced by the number of research documents compiled at Scopus (Elsevier, n.d.) by type of funder - Figure 5, which has undoubtedly been influenced by integrating the Baltic States into these research-funded programmes.

National funding of 28% for research and the Research Council of Norway are also important. The European Union's (EU) Digital Europe Programme fosters digital transformation and the diffusion of digital technologies across the European Union. The programme supports cybersecurity projects that are important for ensuring the security of the state and enterprises.

Figure 5

Main Sources of Funding for Cybersecurity Research in the Baltic States (2012–2024)



Source: Scopus.

Currently, the majority of cybersecurity research in the Baltics is based on EU funding (Horizon 2020 (European Union, 2013), Digital Europe, ERDF) 56%, so it would be valuable to assess the possibilities of diversifying financing, so that the Baltic States are less dependent on EU funds and set country-oriented goals for the research process and invest in strategic research directions that are important for the country. Similar to findings in Craigen et al. (2014), the Baltic region's heavy reliance on EU research funding reflects broader patterns of cybersecurity dependency observed in smaller EU economies.

Conclusions

Based on the bibliometric analysis, policy document research and statistical analysis carried out in the study, it can be concluded that Cybersecurity research in the Baltic States is a growing trend, but its development is still improvable.

1. Estonia is the leader in cybersecurity research in the Baltics, accounting for 54% of all publications (408 out of 756) and demonstrating the highest global Cybersecurity Index (GCI) rating (88.5). This is directly related to the long-term strategy, international cooperation and the development of institutional infrastructure. Lithuania (29% of publications) and Latvia (17%) lag, mainly because they introduced national cybersecurity strategies and institutional research centres much later. ANOVA statistical analysis ($p < 0.05$) confirms significant differences in cybersecurity research activity between the Baltic States.

2. International cooperation and EU funding are key factors in the development of cybersecurity research.

Estonia has actively attracted NATO and EU funding, contributing to its leadership position. NATO's Cooperative Cybersecurity Centre of Excellence (CCDCOE) in Tallinn has significantly contributed to research and international cooperation. The Estonian Centre for Digital Development and the Cyber Training Centre for the Defence Forces also play an important role in research and the development of new technologies.

Latvia and Lithuania rely mostly on EU funds (Horizon Europe, Digital Europe, ERDF) and have yet to develop national funding mechanisms to become more independent from external means.

3. The model of research cooperation between the Baltic States is not yet sufficiently developed.

Scientific cooperation between the Baltic States is not yet optimal, as the research institutions of each country operate in isolation and not as a single regional network.

Potential cooperation models for strengthening the Baltic region are emerging between TalTech (Estonia) and RTU (Latvia) – application of artificial intelligence in cybersecurity, University of Tartu (Estonia) and Vilnius University (Lithuania) – joint research in cryptography and secure communication protocols, Kaunas University of Technology (Lithuania) and Latvia University of Life Sciences and Technologies (LBTU) – cybersecurity of energy and smart electricity grids.

The recommendation is for the Baltic States to develop a common cybersecurity research strategy, including the common use of resources and infrastructure.

4. The sectoral structure of cybersecurity research reveals the importance of multidisciplinarity. Cybersecurity research is not just a matter of computer science or engineering but requires a multidisciplinary approach - Computer science (45%) and engineering (30%) dominate research. In comparison, Social Sciences (10%), psychology (5%) and energy security (10%) are also important factors.

For the Baltic States to prepare more effectively for cyber threats, it is necessary to develop interdisciplinary cooperation involving lawyers, psychologists, and energy experts.

5. The Baltic States must increase their national cybersecurity research contribution.

EU funding accounts for the largest share, or 56% of the research budget in the Baltic States. However, countries must develop funding mechanisms in the long term to ensure independent and stable research and development.

It is vital to increase national investment mechanisms in cybersecurity research through state aid programmes.

Closer collaboration between academic institutions, government agencies, and the private sector is essential to advancing applied research and innovation in cybersecurity. Establishing dedicated funding mechanisms, such as the Baltic Cybersecurity Research Fund, can incentivise joint research initiatives, facilitate knowledge transfer, and accelerate the development of advanced cybersecurity solutions tailored to regional challenges. The integration of the Baltic and European cybersecurity ecosystems should be promoted to strengthen the region's defences against cyberattacks.

References

CERT-LV. (2023). *Latvian cybersecurity and CERT.LV technical activities: Annual report 2023*. Information Technology Security Incident Response Institution of the Republic of Latvia. https://cert.lv/uploads/eng/Annual_Report_CERT-LV_2023.pdf

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4(*10), 13–21. https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf

Deibert, R. & Crete-Nishihata, M. (2011). Blurred boundaries: Probing the ethics of cyberspace research. *Review of Policy Research*, *28*(4), 531–537. https://doi.org/10.1111/j.1541-1338.2011.00529.x

European Union. (2013). *Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020—the Framework Programme for Research and Innovation (2014–2020) and repealing Decision No 1982/2006/EC*. Official Journal of the European Union. https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vjs5ga5ldvzo?utm

European Union. (2021). *EU Strategy for the Baltic Sea Region*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:ev0017

European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Official Journal of the European Union. https://eur-lex.europa.eu/

Elsevier. (n.d.). *Scopus*. Retrieved March 3, 2025, from https://www.scopus.com

Center for Security Studies. (2020). *Estonia's National Cybersecurity and Cyberdefense Posture*. https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/438276/Cyber-Reports-2020-09-Estonia.pdf

International Telecommunication Union. (2024). *Global Cybersecurity Index (GCI) 2024*. https://www.itu.int/pub/D-HDB-GCI.01-2024

Latvian Cabinet of Ministers. (2023). *Latvian Cybersecurity Strategy 2023–2026* [Cabinet Regulation No. 158]. https://www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas%20strategija%202023%20ENG.pdf

Ministry of National Defence of the Republic of Lithuania. (2022). *National Cyber Security Strategy 2022*. https://www.nksc.lt/doc/en/2022_key-trends-and-statistics-of-cyber-security.pdf

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (n.d.). https://ccdcoe.org/

Sandnes, F. E. (2021). A bibliometric study of human–computer interaction research activity in the Nordic-Baltic Eight countries. *Scientometrics*, 126, 4733–4767. https://doi.org/10.1007/s11192-021-03940-z

Szejgiec-Kolenda, B. & Duma, P. (2020). Regional cooperation and governance in the Baltic Sea Region: Implications for the European Union Strategy for the Baltic Sea Region. *Journal of Baltic Studies*, *51*(3), 339–357. https://doi.org/10.1080/01629778.2020.1746889