„Krytyka Prawa", tom 18, nr 2/2026, s. 42–58, ISSN 2080-1084, e-ISSN 2450-7938, © 2026 Authors.

DOMINIK BIERECKI[1], KRZYSZTOF KACZMAREK[2], MIROSŁAW KARPIUK[3]

The Cybersecurity Policy of Poland, Finland, and Sweden and Its Impact on Regional Security[4]

Submitted: 09.03.2026. Accepted: 16.04.2026

Abstract

This article analyses the cybersecurity policy of Poland, Finland, and Sweden within the context of the contemporary European security environment. States operating in a highly digitalised and contested environment increasingly embed cybersecurity within core security policy rather than treating it as a separate technical domain. The analysis draws on selected legal acts and strategic documents and applies a systemic and comparative approach to identify both shared instruments and country-specific institutional solutions. The findings indicate that cybersecurity is closely linked to the protection of critical infrastructure, the continuity of public administration and the ability of institutions to function under conditions of disruption and external pressure. However, differences emerge in how similar assumptions are translated into organisational and coordination mechanisms, reflecting distinct administrative traditions, security cultures and geopolitical positions. The article also shows that NATO membership reinforces the political importance of cybersecurity without fundamentally altering the underlying logic of national policies.

Keywords: national cybersecurity policy, continuity of public administration, Baltic Sea security environment, institutional coordination, Nordic security model.

1 Prof. Dominik Bierecki – Pomeranian University in Słupsk (Poland), e-mail: dominik.bierecki@upsl.edu.pl; ORCID: 0000-0001-6993-3974.

2 Krzysztof Kaczmarek, PhD – Koszalin University of Technology (Poland), e-mail: krzysztof.kaczmarek@tu.koszalin.pl; ORCID: 0000-0001-8519-1667.

3 Prof. Mirosław Karpiuk – University of Warmia and Mazury in Olsztyn (Poland), e-mail: miroslaw.karpiuk@uwm.edu.pl; ORCID: 0000-0001-7012-8999.

4 The research in this article has not been supported financially by any institution.

„Krytyka Prawa", tom 18, nr 2/2026, s. 42–58, ISSN 2080-1084, e-ISSN 2450-7938, © 2026 Author.

DOMINIK BIERECKI, KRZYSZTOF KACZMAREK, MIROSŁAW KARPIUK

Polityka cyberbezpieczeństwa Polski, Finlandii i Szwecji oraz jej wpływ na bezpieczeństwo regionalne[5]

Streszczenie

Niniejszy artykuł analizuje politykę cyberbezpieczeństwa Polski, Finlandii i Szwecji w kontekście współczesnego europejskiego środowiska bezpieczeństwa. Państwa funkcjonujące w silnie zdigitalizowanym i konkurencyjnym środowisku coraz częściej włączają cyberbezpieczeństwo do głównego nurtu polityki bezpieczeństwa, zamiast traktować je jako odrębną dziedzinę techniczną. Analiza opiera się na wybranych aktach prawnych i dokumentach strategicznych oraz wykorzystuje podejście systemowe i porównawcze w celu identyfikacji zarówno wspólnych instrumentów, jak i specyficznych dla poszczególnych krajów rozwiązań instytucjonalnych.

Wyniki wskazują, że cyberbezpieczeństwo jest ściśle powiązane z ochroną infrastruktury krytycznej, zapewnieniem ciągłości funkcjonowania administracji publicznej oraz zdolnością instytucji do działania w warunkach zakłóceń i presji zewnętrznej. Jednocześnie widoczne są różnice w sposobach przekładania podobnych założeń na mechanizmy organizacyjne i koordynacyjne, co odzwierciedla odmienne tradycje administracyjne, kultury bezpieczeństwa oraz uwarunkowania geopolityczne. Artykuł pokazuje również, że członkostwo w NATO wzmacnia polityczne znaczenie cyberbezpieczeństwa, nie zmieniając jednak zasadniczo podstawowej logiki krajowych polityk.

Słowa kluczowe: krajowa polityka cyberbezpieczeństwa; ciągłość działania administracji publicznej, środowisko bezpieczeństwa regionu Morza Bałtyckiego; koordynacja instytucjonalna, nordycki model bezpieczeństwa.

[5] Badania wykorzystane w artykule nie zostały sfinansowane przez żadną instytucję.

 DOI: 10.7206/kp.2080-1084.848

Introduction

Russia's full-scale invasion of Ukraine in February 2022 primarily accelerated and clarified existing dynamics in the European security environment rather than creating an entirely new one. Its significance lay in exposing and intensifying processes that had already been visible in European security debates before 2022 but were often underestimated or politically downplayed. In many European states, the invasion contributed to a delayed recognition of long-standing threats and prompted a gradual abandonment of policies based on avoiding confrontation with Russia and treating it as a predictable partner within the European security order.

This shift was accompanied by a visible weakening of resistance to NATO enlargement and a broader reconfiguration of security priorities in states located along the Alliance's northern and eastern flanks. Sweden and Finland, previously outside formal military alliances, submitted accession applications and subsequently became members of the North Atlantic Treaty Organisation. Poland, already a NATO member, found itself increasingly exposed to intensified pressure as a frontline state bordering both Ukraine and the Russian exclave of Kaliningrad. In response, Russia expanded its spectrum of activities directed against these states, including actions affecting energy infrastructure, telecommunications systems, and the digital domain. These measures illustrate forms of pressure that remain below the threshold of conventional armed conflict while increasingly relying on cyberspace and information operations as instruments of state activity.

In this context, cybersecurity should be understood as an integral component of state security rather than as a narrowly defined technical policy area.[6] It has become closely linked to the protection of critical infrastructure, the continuity of public administration, information systems, and broader social functioning. In Poland, Finland, and Sweden, cybersecurity policies are not implemented exclusively at the national level. International cooperation plays a significant role within the frameworks of the European Union and NATO, while in the Nordic context, it is further reinforced by regional cooperation mechanisms. This multilevel setting creates a complex policy environment in which national institutional solutions intersect with regional arrangements and alliance-based commitments.

[6] D. Bierecki *et al.*, *Sovereignty by Design: Embedding Fiscal Risk Intelligence in Europe's Defence-Digital Strategy*, "Prawo i Więź" 2026, 1, p. 160.

The analysis distinguishes between policy instruments shaped by Nordic regional conditions and those driven primarily by European Union regulations and NATO strategies, while also taking into account Poland's position as a non-Nordic but regionally embedded actor within the same security environment. Particular attention is paid to the ways in which different institutional traditions and security cultures translate shared external pressures into national cybersecurity policies.

This article analyses the cybersecurity policies of Poland, Finland, and Sweden in the evolving European security environment, with particular attention to the role of NATO and the broader regional security context of the Baltic Sea area. It examines how cybersecurity is embedded in state security policy and assesses the extent to which internal resilience and international cooperation influence policy effectiveness across the three cases.

The hypothesis is that in states operating within the Baltic Sea security environment – including Poland, Finland, and Sweden – cybersecurity is embedded in core state security policy and that its effectiveness depends on a combination of internal resilience and extensive international cooperation. To verify this hypothesis, the article examines selected legal and strategic acts related to cybersecurity in all three states. A systemic approach is used to analyse the influence of the international security environment on national policies, while the comparative method allows for the identification of both shared instruments and country-specific solutions that may be relevant in other national contexts.

Cybersecurity threats originating from Russia have consistently disrupted the normal functioning of public institutions in the region, and their intensity has increased significantly since the outbreak of the war in Ukraine. For states neighbouring or geographically close to Russia, it is therefore essential that cybersecurity policies embedded within broader security policy frameworks enable swift and proportionate responses to both cyberattacks and disinformation activities. Achieving this objective requires effective international cooperation, particularly at the regional level, among states directly exposed to Russian cyber and information operations.

Finland and Sweden as Small States in a Highly Digitalised Security Environment

States such as Sweden and Finland are usually classified as small states, taking into account their demographic, economic, and military potential, as well as their

 DOI: 10.7206/kp.2080-1084.848

relatively limited territorial size and resource base.[7] However, this classification does not imply marginal relevance in security terms. In certain areas, particularly those shaped by technological capability rather than scale, these states retain the capacity to influence their regional security environment.[8] One such area is the digital domain. Modern technologies are now embedded in a wide range of social and institutional activities.[9] Advanced digital tools, including artificial intelligence (AI), are no longer confined to specialised sectors but increasingly shape routine state functions. In these conditions, state resilience cannot be addressed through isolated measures. It develops instead through the interaction of technological capacity, administrative organisation, and the ability of societies and institutions to adapt to changing circumstances.[10]

Technological development has altered the role of cybersecurity and data protection within state security.[11] Both have gone beyond a narrow technical understanding and are now closely linked to crisis management practices.[12] At the same time, digital security also concerns the continuity of access to digital services, which remains dependent on the stability of physical infrastructure. Therefore, the relationship between infrastructure security and cybersecurity is reciprocal. Disruptions in one sphere directly affect the other. Damage to energy infrastructure, for example, immediately constrains the functioning of digital services and information systems. This interdependence became visible in autumn 2024, when two fibre-optic telecommunications connections linking Lithuania and Sweden, as well as Finland and Germany, were disrupted. In December of the same year, the EstLink 2 subsea energy cable connecting Finland and Estonia was damaged.[13] These incidents illustrate how physical interference with infrastructure leads to vulnerabilities within the digital environment.

Against this background, the position of Sweden and Finland in EU-level assessments of digital development takes on a different meaning. Both states are

---

7 M. Stănescu, *A Small State's Security Strategy in a Changing World – Republic of Moldova Case Study*, "Scientific Bulletin-Nicolae Balcescu Land Forces Academy" 2024, 2, p. 308.

8 M. Malužinas, *The Role of Small States in Promoting International Security: Lithuania Strategy*, "Przegląd Strategiczny" 2023, 16, p. 164.

9 E. M. Włodyka, *Implementation of e-Government and Artificial Intelligence in Polish Public Administration*, "TalTech Journal of European Studies" 2024, 2, p. 120.

10 K. Kaczmarek, *Bezpieczeństwo państwa wobec współczesnych zagrożeń*, „Prawo i Więź" 2025, 5, p. 577.

11 K. Kaczmarek *et al.*, *A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data*, "Prawo i Więź" 2024, 3, p. 105.

12 K. Kaczmarek *et al.*, *The Status of Government Administration in the Sphere of Crisis Management*, "Prawo i Więź" 2025, 6, p. 666.

13 R. Miętkiewicz, *Zagrożenia hybrydowe na Morzu Bałtyckim. Wyniki analizy możliwości przeciwdziałania*, [in:] K. Wojtasik, D. Szlachter, *Zagrożenia terrorystyczne i sabotażowe infrastruktury krytycznej*, Warszawa 2025, p. 38.

commonly placed among the most digitally advanced in the Union. This standing does not result from a single dominant element but from the long-term combination of digital skills, network infrastructure, and the extensive use of digital solutions in public administration.[14] At the same time, this level of digitalisation has produced a structural dependence on the uninterrupted functioning of information and communication systems, particularly in areas central to public governance and critical infrastructure.

Importantly, the digital paths followed by Sweden and Finland do not suggest unrestricted technological expansion. Adoption remains selective and regulated. Public authorities continue to play a decisive role in the definition of standards, limits, and safeguards. From this perspective, cybersecurity appears less as a separate policy sector and more as a practical condition for the continued operation of state functions embedded in a digital environment, closely linked to resilience and cooperation beyond the national level.[15] These structural conditions form the background against which cybersecurity policies in the Nordic context can be analysed prior to examining state-level responses.

The Nordic Approach to Digital Security and State Resilience

In the Nordic region, cybersecurity is generally discussed in direct connection with the continuity of essential services and the ability of society to function under stress. In Finland, this is expressed through the comprehensive security model described in the Security Strategy for Society (*Yhteiskunnan turvallisuusstrategia*), which treats preparedness as joint work carried out by public authorities, businesses, organisations, and citizens. The document is explicit about 'vital functions' and shared responsibility: it is not written as a narrow IT policy.[16] A similar logic can be seen in the Swedish policy language, where cybersecurity is tied to the functioning of society and the protection of key values. The Swedish Government's *National Cyber Security Strategy* links cyber dependency to broader security goals and explicitly

[14] *The Digital Economy and Society Index (DESI)*, The European Commission, accessed January 7, 2026. Available from: https://digital-strategy.ec.europa.eu/en/policies/desi.

[15] M.S. Jensen, *Cyberresiliens, sektorprincip og ansvarsplacering – nordiske erfaringer*, "Internasjonal Politikk" 2019, 3, pp. 270–271, 273–275.

[16] Valtioneuvosto (Government of Finland), *Yhteiskunnan turvallisuusstrategia*, Valtioneuvoston periaatepäätös, Valtioneuvoston julkaisuja 2025:1 (2025), https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/817eb584-f510-49a2-ad2f-9106226b2f20/content.

 DOI: 10.7206/kp.2080-1084.848

connects cybersecurity with social functioning. It does not treat cyberspace as a niche sector with purely technical aims.[17]

This approach also appears in how continuity is handled in practice. In Sweden, the Civil Contingencies Agency (MSB) presents continuity management as a tool for maintaining samhällsviktig verksamhet (societally important activities) even under increased preparedness and, ultimately, war. The key message is straightforward: if electricity, IT systems, or supply chains fail, critical functions still have to operate. This is continuity planning written for practitioners rather than for theoretical discussion.[18] Finland's updated Cyber Security Strategy 2024–2035 fits the same pattern. It is drafted as a state-level document but built around coordination, responsibilities, and the operating environment rather than technology alone. It explicitly links the strategy to EU requirements such as NIS2 and embeds it within broader national and international security planning.[19]

Nordic cooperation strengthens this 'continuity + coordination' way of thinking. In the Nordic–Baltic format, digitalisation is treated as a shared policy space, with clear priorities for mobility, interoperability, skills, and secure digital public services. The Nordic-Baltic Cooperation Programme for Digitalisation 2025–2030 is relevant here because it connects integration goals with capacity, competence, and security-related issues across borders.[20] A concrete example of cooperation is the regional focus on critical subsea infrastructure. In a joint statement, the Nordic and Baltic ministers of digitalisation highlight the security of subsea communication cables and the need for stronger cooperation around protection and resilience. This directly supports the link between infrastructure security and digital security without reducing it to a general slogan.[21]

Finally, Nordic cooperation also exists as a security-policy format, not only as sectoral coordination. The N5 (Nordic) and NB8 (Nordic–Baltic) formats are described by the Swedish Government as informal cooperation frameworks for foreign

---

17 Government of Sweden, *A National Cyber Security Strategy*, Government Communication to Riksdag, Skr. 2016/17:213 (Stockholm, June 22, 2017). Available from: https://www.government.se/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213.

18 *Kontinuitetshantering – en viktig del i arbetet med samhällsskydd och beredskap*, Myndigheten för samhällsskydd och beredskap (MSB), publ. nr MSB1415, March 2019. Available from: https://rib.msb.se/filer/pdf/29043.pdf

19 *Finland's Cyber Security Strategy 2024–2035*, Publications of the Prime Minister's Office 2024:13 (Prime Minister's Office, Helsinki, 2024).

20 Nordic Council of Ministers, *Nordic-Baltic Cooperation Programme for Digitalisation 2025–2030* (Copenhagen: Nordic Council of Ministers, 2024).

21 Nordic Council of Ministers, "Joint Statement by the Nordic and Baltic Ministers for Digitalisation on Cooperation in the Protection of Critical Subsea Infrastructure," Nordic Council of Ministers, issued November 2024. Available from: https://www.norden.org/en/declaration/joint-statement-nordic-and-baltic-ministers-digitalisation.

and security policy, with regular meetings and a dense calendar of working-level contacts. For this cooperation serves practical purposes, as it helps explain why "cooperation beyond the national level" is treated as routine rather than exceptional.[22]

Taken together, these documents show a consistent regional tendency: cybersecurity is framed in terms of continuity, essential services, and shared responsibility, while cross-border cooperation is treated as a normal part of preparedness. This provides the background for the next stage of the analysis, which moves from the regional level to the national level and examines how Sweden and Finland translate these assumptions into concrete cybersecurity policies.

Organisation and Coordination of Cybersecurity in Finland and Sweden

In Finland, cybersecurity policy is shaped through long-term planning at the government level. The current framework covers more than one political cycle and is treated as a stable element of state activity. It is also updated on a regular basis. Not only 'when something happens'. There is a planned pattern of revision and follow-up.[23] The strategy is paired with an implementation plan. This is important in practice. It is not merely a list of objectives. The plan assigns tasks and indicates who is responsible. It also assumes regular monitoring and evaluation.[24] Consequently, the policy is not left as a purely declaratory instrument. It is intended to guide practical implementation and policy development.

Operational coordination is carried out within the transport and communications administration. A specialised national centre operates within this structure and is responsible for monitoring, information exchange, and incident-related activities. It performs functions that extend beyond basic technical support. It contributes to situational awareness and disseminates information.[25] This may take the form of alerts. It may also take the form of guidance. The objective is to maintain a shared understanding of the evolving situation. Incident response is organised through a dedicated national team within that structure. Reports are

---

22 Government of Sweden, "N5 and NB8 – Nordic and Nordic-Baltic Cooperation on Foreign and Security Policy," Government Offices of Sweden Available from: https://www.government.se/government-policy/n5-and-nb8--nordic-and-nordic-baltic-cooperation-on-foreign-and-security-policy/ (accessed: 7.01.2026).

23 M. Lehto, J. Limnéll, *Strategic leadership in cyber security, case Finland*, "Information Security Journal: A Global Perspective" 2021, 3, pp. 42–43.

24 L. Jauhiainen, S. Schiffling, *Comparing the resilience objectives of Finnish comprehensive security model and the NATO baseline requirements for resilience*, "Journal of Military Studies" 2025, 1, pp. 9–10.

25 J. Pöyhönen *et al.*, *Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations*, "Information & Security: An International Journal" 2019, 2, p. 237.

 DOI: 10.7206/kp.2080-1084.848

collected and processed. Patterns are analysed.[26] The framework also includes cooperation with international partners and information sharing. The structure is designed to remain operational under conditions of pressure. It provides a central reporting point and a single touchpoint for enquiries. This reduces institutional complexity and fragmentation.

The legal changes introduced in 2025 expanded the scope of cybersecurity obligations. More entities are covered. Compliance is not presented as optional. It imposes specific obligations. Risk management is one of them. Reporting is another. The underlying logic is one of organisational responsibility. It is not about writing technical manuals into law. Supervision is part of the design as well, so obligations are not only symbolic.[27]

Some duties start with a basic step that is easy to miss. The first requirement is registration. This entails formal inclusion within the relevant regulatory framework.[28] This is administrative, not technical. Still, it changes the relationship between the state and the entity. The relationship shifts from voluntary good practice to a formal legal obligation. This is followed by the introduction of internal organisational measures, which include documented procedures, leadership-level training, and specific implementation deadlines. Not all at once, but the direction is clear.

In Sweden, cybersecurity policy is presented somewhat differently. More specifically, it is articulated through government communications to Parliament.[29] These documents set priorities and signal what the government expects. They do not read like a manual. Instead, they function primarily as instruments of policy direction. Cybersecurity is treated as a condition for the functioning of essential services and public administration. That is the core framework. There is also a strong link to national security and crisis preparedness. Cybersecurity is not described as a separate field with its own logic. It is integrated into the wider security architecture.[30] Continuity is a recurring theme, and particular emphasis

---

26 Kyberturvallisuuskeskus, "CERT". Available from: https://kyberturvallisuuskeskus.fi/en/our-activities/cert (accessed: 9.02.2026).

27 Traficom, "Cybersecurity Act passed by Parliament, obligations under the NIS 2 Directive enter into force 8 April 2025", *Traficom*, April 8, 2025. Available from: https://traficom.fi/en/news/cybersecurity-act-passed-parliament-obligations-under-nis-2-directive-enter-force-8-april-2025.

28 S. Schmitz-Berndt, M. Cole, *Towards an Efficient and Coherent Regulatory Framework on Cybersecurity in the EU: The Proposals for a NIS 2.0 Directive and a Cyber Resilience Act*, "Applied Cybersecurity & Internet Governance" 2022, 1, p. 9.

29 Riksdagen, "Nationell strategi för cybersäkerhet 2025–2029", Skrivelse 2024/25:121, submitted March 20, 2025. Available from: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/skrivelse/nationell-strategi-for-cybersakerhet-2025-2029_hc03121/.

30 Government of Sweden, "Cybersecurity", Government Offices of Sweden. Available from: https://www.government.se/government-policy/cybersecurity/ (accessed: 9.02.2026).

is placed on maintaining functionality during disruptions. The central idea that the state must continue to function even when systems are under stress.

Coordination is another significant factor. Sweden does not build everything around an operational centre that 'owns' the whole field. The model is more about joining institutions and building a platform for cooperation. This is where the national cybersecurity centre fits in. It started as a cooperation arrangement between authorities. Then it was reorganised with the aim of raising ambition and tightening leadership. It is meant to become a hub. However, this does not imply a single command structure replacing existing agencies. Rather, it operates as a structured mechanism for inter-agency cooperation.

This institutional choice affects the style of policy. Greater emphasis is placed on joint action and harmonising routines. It also includes enhanced information sharing. The objective is to improve coordination among agencies. Formal decisions were taken to move parts of the cybersecurity activity to a stronger organisational host.[31] This is not a small administrative tweak. It changes leadership, resources, and expectations. Regulatory changes related to the implementation of new EU requirements introduce additional obligations in Sweden as well. Registration again appears as a practical threshold. Then there are organisational measures and incident reporting. Some sectors communicate them in plain language. And these requirements are presented in practical rather than theoretical terms, i.e. often as concrete obligations, including registration, security measures, training, and reporting. Such measures are intended to influence organisational behaviour. The result is a system characterised by stronger obligations, greater institutional structure, and less reliance on voluntary compliance. But institutional tools are not identical. Finland relies on long planning horizons and a central operational structure with clear contact points.[32] Sweden places more weight on political steering and inter-agency coordination, with a centre designed to connect authorities and raise the level of joint action. In both cases, cybersecurity policy is tied to state functioning. And it is most definitely not treated as a narrow technical issue.

---

31 Swedish Government (Regeringskansliet), *Ett nytt Nationellt cybersäkerhetscenter: Ändamålsenliga och effektiva former för ledning, organisering och styrning. Del 1*. Available from: https://www.regeringen.se/contentassets/73f464426acc4c8da2b342a2eb91d627/ett-nytt-nationellt-cybersakerhetscenter---del-1/ (accessed: 9.02.2026).

32 M.K. Griffith, *A Comprehensive Security Approach: Bolstering Finnish Cybersecurity Capacity*, "Journal of Cyber Policy" 2018, 3, pp. 410–415.

 DOI: 10.7206/kp.2080-1084.848

Poland's Cybersecurity Policy

Due to its geographical proximity to Russia, Poland is exposed to an elevated level of cyber activity originating from that state. Threats emerging in cyberspace may significantly undermine not only economic stability but also the state security system, which relies to a considerable extent on digital solutions and information technologies.

Poland's cybersecurity policy is based on a national cybersecurity strategy.[33] According to this strategy, the successful development of the state, the growth of its resources, economic efficiency, the effective functioning of public institutions and private entities, as well as social activity, are closely linked to the reliable and secure operation of information systems and electronic communication networks. Consequently, the state is required to systematically strengthen and develop the national cybersecurity system. Measures in this area should encompass comprehensive organisational, operational, technological, and legal solutions, as well as the shaping of social attitudes and the promotion of scientific research, in order to ensure high cybersecurity standards in the field of software, digital devices, and services. These actions must be undertaken with full respect for citizens' rights and freedoms.[34] At the same time, the state is expected to foster trust between market sectors and public administration. One of the objectives of Poland's cybersecurity strategy is to strengthen the country's international position in the field of cybersecurity, which necessitates active international cooperation at both the strategic-political and operational-technical levels.

In the context of globalisation and the resulting interdependencies between states, international cooperation constitutes a fundamental condition for ensuring the security of global cyberspace.[35] The development of a secure global digital

---

33 Cybersecurity Strategy of the Republic of Poland for 2019–2024, constituting an annex to Resolution No. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019–2024 (Monitor Polski 2019, item 1073). On cybersecurity, see also: P. Krauze-Maślankowska, D. Majewicz, *Cybersecurity in the Development of Smart Cities: A Big Data Analysis of Digital Security Management Practices by Local Public Administration in Poland*, "Ius et Securitas" 2025, 2; D. Bierecki *et al.*, *Security in the Era of Cybersecurity Threats*, "Prawo i Więź" 2025, 4; C. Gaie *et al.*, *Cybersecurity of Public Sector Institutions*, "Prawo i Więź" 2024, 6; M. Czuryk, *Jurisdiction of the Voivode in the Field of Crisis Management*, "Studia Iuridica Lublinensia" 2025, 1 pp. 94–95; T. Wojciechowski, *Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego*, „Ius et Securitas" 2024, 1.

34 On the protection of human and civil rights and freedoms, see: M. Czuryk, *Dopuszczalne różnicowanie sytuacji pracowników ze względu na religię, wyznanie lub światopogląd*, „Studia z Prawa Wyznaniowego" 2024, 27.

35 *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, Warszawa 2017, p. 24.

environment cannot take place without coherent regional cybersecurity policies, particularly in light of the ongoing war in Ukraine.

The development of information and communication technologies and the expansion of the Internet have generated new external threats, including cyber crises and cyber conflicts involving both state and non-state actors, as well as the risk of cyber warfare. Operations conducted in cyberspace have become an integral component of contemporary political and military crises and conflicts, contributing to their hybrid character. A particularly significant external threat in cyberspace is cyber espionage, carried out by foreign intelligence services and non-state actors, including terrorist organisations, using specialised tools to gain access to data of strategic importance to the state.[36] At present, cyber espionage activities conducted by Russia appear to be intensifying, with the aim of destabilising states in the region. This makes international cooperation essential in countering such activities.

Polish strategic documents emphasise the need to enhance resilience to cyber threats and to strengthen the protection of information across the public, military, and private sectors, as well as to promote knowledge and good practices that enable citizens to better safeguard their personal and professional data.[37]

Like Finland and Sweden, Poland must take into account the norms and principles applicable within the European Union when shaping its cybersecurity policy, including those related to risk management. Threats to the security of networks and information systems may originate from various sources. Therefore, cybersecurity risk management measures should address the full spectrum of threats, as their purpose is to protect both information systems and their physical environment against incidents such as theft, fire, flooding, telecommunications failures, power outages, or unauthorised physical access to information infrastructure. Such incidents may compromise the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data, as well as the continuity of services provided through information systems. Consequently, cybersecurity risk management measures must also address physical security. Appropriate safeguards should be implemented to protect networks and information systems against technical failures, human error, malicious actions, and natural phenomena. Particular attention should also be paid to human resources security, including the implementation of adequate access control policies.[38]

---

36 *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015, pp. 12–13.

37 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2020, p. 20.

38 Recital 79 of 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27 December 2022, pp. 80–152.

 DOI: 10.7206/kp.2080-1084.848

Cyberattacks are often transboundary in nature; however, the competencies and political responses of authorities responsible for cybersecurity and law enforcement remain predominantly national. It should be emphasised that large-scale incidents may disrupt the provision of essential services across the European Union. Such situations require effective and coordinated responses and crisis management at the EU level, based on dedicated policy instruments as well as broader mechanisms of European solidarity and mutual assistance. Regular assessments of the state of cybersecurity and resilience within the EU, grounded in reliable data, along with systematic forecasting of future changes, challenges, and threats at both the European and global levels, are therefore of considerable importance for political decision-makers, industry stakeholders, and users.[39] Cooperation at the EU level does not preclude collaboration within the Baltic Sea region, which may also contribute to limiting Russia's capacity to conduct cyberattacks against other EU member states.

Initiatives aimed at enhancing cooperation with other states in order to more effectively counter cyberattacks must be accompanied by the development of national capabilities enabling the prevention of cyber threats, effective response measures, and the rapid mitigation of their effects. Accordingly, investment in national cybersecurity systems is necessary so that they can serve as a foundation for countering cyberattacks of a smaller scale.

Polish legislation defines the national cybersecurity system as a framework designed to ensure cybersecurity at the national level, primarily by guaranteeing the uninterrupted provision of essential and digital services. This objective is pursued by achieving an appropriate level of security for information systems used in the provision of such services and by ensuring effective incident-handling mechanisms.[40] The legal definition therefore focuses on the security of information systems, which currently constitute the operational foundation of many entities, including public institutions.

Conclusions

The article aimed to examine how cybersecurity policies operate in Poland, Sweden, and Finland in the current European security environment, with particular attention to the role of NATO and the place of cybersecurity within state security

[39] Recital 5 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification, and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7 June 2019, pp. 15–69.

[40] Article 3 of the Act of 5 July 2018 on the national cybersecurity system (Journal of Laws of 2026, item 20).

policy. This perspective makes it possible to move beyond a purely technical reading of cybersecurity and to focus instead on how it is organised, governed, and embedded in broader security thinking.

The analysis shows that in all three states, cybersecurity is treated as part of core state activity. It is closely linked to the continuity of public administration, the protection of critical infrastructure, and the ability of institutions to operate under pressure. Cybersecurity does not appear as a separate policy field with its own autonomous logic. Instead, it is integrated into state security arrangements and embedded in everyday governance practices.

This observation is important for the hypothesis formulated in the introduction. The material examined indicates that the effectiveness of cybersecurity policies in Poland, Sweden, and Finland is not based solely on technical capacity. It depends on institutional resilience, legal clarity, and the ability to coordinate actions across sectors and levels of governance. International cooperation plays a visible role in this process. European Union regulations and NATO membership form part of the normal operating environment of national policies, while in the Nordic context, this is further reinforced by regional cooperation frameworks.

At the same time, the comparison highlights differences in the way similar assumptions are translated into institutional solutions. Finland relies on long-term strategic planning and a centralised operational structure with clearly defined responsibilities. Sweden places a greater emphasis on political steering and coordination between authorities, embedding cybersecurity within wider crisis management and national security frameworks. Poland, operating as a frontline state on the eastern flank of NATO and the European Union, places particular emphasis on legal frameworks, institutional coordination, and the protection of public-sector information systems against persistent external pressure. These differences do not undermine policy coherence. They reflect administrative traditions, security cultures, and geopolitical positioning.

The analysis also suggests that NATO has not fundamentally transformed the core logic of cybersecurity policies in any of the three states. Instead, alliance membership has reinforced existing trends and increased the political weight of cybersecurity within state security policy. Cybersecurity has become more clearly associated with credibility, preparedness, and alliance participation, while its basic institutional logic has remained intact.

From this perspective, the cases of Poland, Sweden, and Finland illustrate how states operating in a highly digitalised and contested regional security environment address security challenges through organisation, coordination, and cooperation rather than through scale alone. Cybersecurity policy emerges not as a response

 DOI: 10.7206/kp.2080-1084.848

to isolated threats but as an element of state capacity and resilience in a complex and interconnected security environment.

References

Act of 5 July 2018 on the national cybersecurity system (Poland) (Journal of Laws of 2026, item 20).

Bierecki D., Czuryk M., Gaie C., Langlois-Berthelot J., *Sovereignty by Design: Embedding Fiscal Risk Intelligence in Europe's Defence-Digital Strategy*, "Prawo i Więź" 2026, 1. https://doi.org/10.36128/2z2k7566

Bierecki D., Karpiuk M., Melchior C., Strizzolo N., *Security in the Era of Cybersecurity Threats*, "Prawo i Więź" 2025, 4. https://doi.org/10.36128/PRIW.VI57.1476

Cybersecurity Strategy of the Republic of Poland for 2019–2024, constituting an annex to Resolution No. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019–2024 (Monitor Polski 2019, item 1073).

Czuryk M., *Dopuszczalne różnicowanie sytuacji pracowników ze względu na religię, wyznanie lub światopogląd*, „Studia z Prawa Wyznaniowego" 2024, 27. https://doi.org/10.31743/spw.17518

Czuryk M., *Jurisdiction of the Voivode in the Field of Crisis Management*, "Studia Iuridica Lublinensia" 2025, 1. https://doi.org/10.17951/sil.2025.34.2.87-98

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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union L 333 (27 December 2022): 80–152.

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej, Warszawa 2015.

Gaie C., Karpiuk M., Strizzolo N., *Cybersecurity of Public Sector Institutions*, "Prawo i Więź" 2024, 6. https://doi.org/10.36128/PRIW.VI53.1129

Government of Sweden. "Cybersecurity". Government Offices of Sweden. Accessed February 9, 2026. Available from: https://www.government.se/government-policy/cybersecurity/

Government of Sweden. "N5 and NB8 – Nordic and Nordic-Baltic Cooperation on Foreign and Security Policy." Government Offices of Sweden. Available from: https://www.government.se/government-policy/n5-and-nb8--nordic-and-nordic-baltic-cooperation-on-foreign-and-security-policy/ (accessed: 7.01.2026).

Government of Sweden. *A National Cyber Security Strategy*. Government Communication to Riksdag, Skr. 2016/17:213. Stockholm, 2017. Available from: https://www.government.se/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213

Griffith M.K., *A Comprehensive Security Approach: Bolstering Finnish Cybersecurity Capacity*, "Journal of Cyber Policy" 2018, 3. https://doi.org/10.1080/23738871.2018.1561919

Jauhiainen L., Schiffling S., *Comparing the resilience objectives of Finnish comprehensive security model and the NATO baseline requirements for resilience*, "Journal of Military Studies" 2025, 1. https://doi.org/10.2478/jms-2025-0003

Jensen M.S., *Cyberresiliens, sektorprincip og ansvarsplacering – nordiske erfaringer*, "Internasjonal Politikk" 2019, 3. http://dx.doi.org/10.23865/intpol.v77.1369

Kaczmarek K., *Bezpieczeństwo państwa wobec współczesnych zagrożeń*, „Prawo i Więź" 2025, 5. https://doi.org/10.36128/PRIW.VI58.1382

Kaczmarek K., Karpiuk M., Melchior C., *A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data*, "Prawo i Więź" 2024, 3. https://doi.org/10.36128/PRIW.VI50.907

Kaczmarek K., Włodyka E.M., Czuryk M., *The Status of Government Administration in the Sphere of Crisis Management*, "Prawo i Więź" 2025, 6. https://doi.org/10.36128/48wmzt46

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022. Warszawa 2017.

Krauze-Maślankowska P., Majewicz D., *Cybersecurity in the Development of Smart Cities: A Big Data Analysis of Digital Security Management Practices by Local Public Administration in Poland*, "Ius et Securitas" 2025, 2.

Kyberturvallisuuskeskus. "CERT." Available from: https://kyberturvallisuuskeskus.fi/en/our-activities/cert (accessed: 9.02.2026).

Lehto M., Limnéll J., *Strategic leadership in cyber security, case Finland*, "Information Security Journal: A Global Perspective" 2021, 3. https://doi.org/10.1080/19393555.2020.1813851

Malužinas M., *The Role of Small States in Promoting International Security: Lithuania Strategy*, "Przegląd Strategiczny" 2023, 16. https://doi.org/10.14746/ps.2023.1.11

Miętkiewicz R., *Zagrożenia hybrydowe na Morzu Bałtyckim. Wyniki analizy możliwości przeciwdziałania*, [in:] K. Wojtasik, D. Szlachter, *Zagrożenia terrorystyczne i sabotażowe infrastruktury krytycznej*, Warszawa 2025.

Myndigheten för samhällsskydd och beredskap (MSB). *Kontinuitetshantering – en viktig del i arbetet med samhällsskydd och beredskap*. Publ. nr MSB1415. March 2019. https://rib.msb.se/filer/pdf/29043.pdf.

Nordic Council of Ministers. "Joint Statement by the Nordic and Baltic Ministers for Digitalisation on Cooperation in the Protection of Critical Subsea Infrastructure." Nordic Council of Ministers. November 2024. https://www.norden.org/en/declaration/joint-statement-nordic-and-baltic-ministers-digitalisation

Nordic Council of Ministers. *Nordic-Baltic Cooperation Programme for Digitalisation 2025–2030*. Copenhagen, 2024. https://doi.org/10.6027/politiknord2024-754

Pöyhönen J., Nuojua V., Lehto M., Rajamäki J., *Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations*, "Information & Security: An International Journal" 2019, 2. https://doi.org/10.11610/isij.4318

Prime Minister's Office. *Finland's Cyber Security Strategy 2024–2035*. Publications of the Prime Minister's Office 2024:13. Helsinki, 2024.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification, and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union L 151 (7 June 2019): 15–69.

Riksdagen. "Nationell strategi för cybersäkerhet 2025–2029". Skrivelse 2024/25:121. Submitted March 20, 2025. Available from: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/skrivelse/nationell-strategi-for-cybersakerhet-2025-2029_hc03121/.

Schmitz-Berndt S., Cole M., *Towards an Efficient and Coherent Regulatory Framework on Cybersecurity in the EU: The Proposals for a NIS 2.0 Directive and a Cyber Resilience Act*, "Applied Cybersecurity & Internet Governance" 2022, 1. https://doi.org/10.5604/01.3001.0016.1323

Stănescu M., *A Small State's Security Strategy in a Changing World – Republic of Moldova Case Study*, "Scientific Bulletin-Nicolae Balcescu Land Forces Academy" 2024, 2. https://doi.org/10.2478/bsaft-2024-0031

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Warszawa 2020.

Swedish Government (Regeringskansliet). *Ett nytt Nationellt cybersäkerhetscenter: Ändamålsenliga och effektiva former för ledning, organisering och styrning. Del 1*. Available from: https://www.regeringen.se/contentassets/73f464426acc4c8da2b342a2eb91d627/ett-nytt-nationellt-cybersakerhetscenter---del-1/ (accessed: 9.02.2026).

The European Commission, *The Digital Economy and Society Index* (*DESI*), Available from: https://digital-strategy.ec.europa.eu/en/policies/desi (accessed: 7.01.2026).

Traficom, "Cybersecurity Act passed by Parliament, obligations under the NIS 2 Directive enter into force 8 April 2025." *Traficom*, April 8, 2025. Available from: https://traficom.fi/en/news/cybersecurity-act-passed-parliament-obligations-under-nis-2-directive-enter-force-8-april-2025

Valtioneuvosto (Government of Finland). *Yhteiskunnan turvallisuusstrategia*. Valtioneuvoston periaatepäätös. Valtioneuvoston julkaisuja 2025:1. 2025. Available from: https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/817eb584-f510-49a2-ad2f-9106226b2f20/content

Włodyka E.M., *Implementation of e-Government and Artificial Intelligence in Polish Public Administration*, "TalTech Journal of European Studies" 2024, 2. https://doi.org/10.2478/bjes-2024-0019

Wojciechowski T., *Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego*, „Ius et Securitas" 2024, 1.