Dmytro Beseda
PhD at the National Academy of the Security Service of Ukraine
besedadmytro24@gmail.com
Piotr Kusznieruk
Full Doctor, Dean of the Faculty of Social Sciences, Warsaw Medical Academy
p.kusznieruk@outlook.com
Galyna Karelova
Researcher at the Department of Law Enforcement and Anti-Corruption Activities, Interregional Academy of Personnel Management
g-karelova@hotmail.com
Mykola Pogrebytskyi
Full Doctor, Professor at the National Academy of the Security Service of Ukraine
m_pogrebytskyi@outlook.com
Olena Kravchenko
PhD, Researcher at the National Academy of the Security Service of Ukraine
olkravchenko@hotmail.com

Comparative study of governmental approaches to the security of critical information systems

Abstract

The aim of this study is to conduct a comparative analysis of national strategies and legal mechanisms for the protection of critical information systems in Poland, the Netherlands, Ukraine, and Canada. The research methodology is based on a theoretical analysis of national legislative acts, strategic documents, and international reports, which enabled the systematisation and comparison of institutional and regulatory approaches. It was found that despite common challenges – such as the rising number of cyber threats, reported by 72% of organisations, and the significant impact of incidents on 59% of companies – the examined countries have developed three distinct protection models. Poland and the Netherlands exemplify a European approach focused on the implementation of EU directives, which aim at harmonising requirements and creating a unified market for cybersecurity services. Ukraine's model, shaped by wartime conditions, is centred on military cyber defence and crisis response. Canada's model, where 51% of public cybersecurity investments are allocated at the

provincial level, is characterised by federal partnerships and decentralisation. The study confirmed that the key issues for all countries remain the shortage of qualified personnel – as 47% of EU operators do not plan to expand their staff – and a significant disparity in security maturity, with 90% of companies being technically unprepared to face modern threats. The practical significance of the study lies in its potential to inform the improvement of national cybersecurity policies through the synthesis of practices from different regulatory models, thereby contributing to the development of more resilient and adaptive national protection systems capable of effectively countering both state and non-state cyber threats.

Keywords: Cyber Resilience – State Regulation – Public-Private Partnership – Operators of Essential Services – Digital Transformation

1. Introduction

In the context of rapid digital transformation, the security of critical information systems has become a matter of fundamental importance for both national and international security. The proliferation of Internet of Things (IoT) technologies, smart cities, and cloud computing has profoundly reshaped not only economic processes but also the structure of public administration and the provision of public services. Alongside undeniable benefits, such as increased efficiency and improved quality of life, this technological evolution has generated new and unprecedented challenges. As Ma[1] noted, the vulnerability of a single element in a smart city system can jeopardise the entire urban ecosystem, from energy supply to transportation and healthcare. This dependency on information and communication technologies (ICT) has rendered cyberspace not only a domain for cybercrime but also an arena for geopolitical confrontation, where critical infrastructure becomes a primary target of malicious attacks.

1 C. Ma, *Smart city and cyber-security; technologies used, leading challenges and future recommendations*, in *Energy Reports*, 2021, Vol. 7, pp. 7999-8012.

The academic discourse on critical infrastructure cybersecurity is developing along several key directions. A significant body of research is devoted to the development and analysis of various security frameworks and standards. Taherdoost[2], in his review, noted the existence of a wide range of standards developed by different organisations, and emphasised that the main challenge for businesses and public institutions lies in choosing the most relevant approach. He highlighted that the absence of a universal standard creates a "paradox of choice", where organisations are forced to choose among dozens of models without clear criteria for evaluating their effectiveness in a specific context. Another approach, which stresses the importance of a holistic perspective, was proposed by Judijanto et al.[3], who argued that Enterprise Architecture plays a crucial role in reducing business risks. In their view, integrating cybersecurity into the overall organisational strategy – rather than treating it as a standalone technical function – enables synergies and ensures resilience across all levels of governance.

Beyond strategic frameworks, scholars also examine legal and organisational measures. This institutional dimension is further emphasised by Blyznyuk et al.[4] who demonstrated that the success of digital transformation projects in public administration depends critically on institutional capacity, governance practices, and risk management capabilities – factors equally relevant to the implementation of cybersecurity measures. Boranbayev et al.[5] studied mechanisms to ensure the reliability of public and critical information systems, emphasising the need for a combination of organisational (security policies, staff training), technical (protective tools), and legal (regulatory requirements, liability) instruments.

---

2 H. Taherdoost, *Understanding cybersecurity frameworks and information security standards – A review and comprehensive overview*, in *Electronics*, 2022, Vol. 11, No. 14, p. 2181.

3 L. Judijanto, D. Hindarto, S. I. Wahjono, Djunarto, Edge of enterprise architecture in addressing cyber security threats and business risks. *International Journal Software Engineering and Computer Science*, 2023, Vol. 3, No. 3, pp. 386-396.

4 A. Blyznyuk, I. Melnyk, Yu. Hrinchenko, A. Solomko, S. Lernyk, O. Moshak, *Formation the project maturity of public administration in implementation of digital transformation projects*, in *Journal of Information Technology Management*, 2021, Vol. 13, pp. 163-187.

5 A. Boranbayev, S. Boranbayev, A. Nurbekov, *Measures to ensure the reliability of the functioning of information systems in respect to state and critically important information systems*, in K. Arai, S. Kapoor, R. Bhatia (Eds.), *Intelligent Systems and Applications: Proceedings of the 2020 Intelligent Systems Conference,* Springer, 2021, pp. 139-152.

They argued that none of these elements is sufficient on its own, and the effectiveness of a system depends on their synergy and comprehensive implementation. Similar conclusions were reached by Bondarenko et al.[6], who analysed the legal mechanisms for information security in the broader context of digitalisation. The authors argued that a comprehensive system of legal norms, combined with effective enforcement and alignment with international standards, is essential for ensuring resilience and trust in digital governance. They highlighted that fragmented or outdated legislation may become a critical vulnerability, undermining even the most advanced technical safeguards.

An important aspect reflecting the European approach is the analysis of EU regulatory acts. The works of Chałubińska-Jentkiewicz and Nowikowska[7] and Mączka[8] provided a detailed examination of the provisions of the EU's Network and Information Security Directive, also known as NIS2. These authors considered the Directive not merely as a technical standard but as a comprehensive practical guide for implementing information security management systems, establishing clear requirements for risk assessment, incident reporting, and supply chain protection for operators of essential services. At the same time, scholarly literature places considerable emphasis on the human factor. As demonstrated in the systematic review by Khando et al.[9], purely technological measures are insufficient, as a significant number of incidents are attributed to human error or negligence. The authors concluded that investments in enhancing Information Security Awareness (ISA) among personnel are as crucial as investments in technical safeguards, since staff serve as the "first line of defence". Separate studies focus on the analysis of national cybersecurity systems, which is especially valuable for comparative analysis. For

6 S. Bondarenko, O. Makeieva, O. Usachenko, V. Veklych, T. Arifkhodzhaieva, S. Lernyk, *The legal mechanisms for information security in the context of digitalization*, in *Journal of Information Technology Management*, 2022, Vol. 14, pp. 25-58.

7 K. Chałubińska-Jentkiewicz, M. Nowikowska, *Entities involved in the policy of ensuring the security of networks and information systems in the light of the NIS2 Directive (part 2)*, in *Cybersecurity and Law*, 2024, Vol. 12. No. 2, pp. 5-24.

8 K. Mączka, *The NIS2 Directive as a guideline for implementing an information security management system in an organization,* in *Protection of People and Cultural Heritage*, 2024, Vol. 5, pp. 111-124.

9 K. Khando, S. Gao, S. M. Islam, A. Salman, *Enhancing employees information security awareness in private and public organisations: A systematic literature review*, in *Computers & security*, 2021, Vol. 106, article no. 102267.

example, Ojdana-Kościuszko[10] analysed the evolution and challenges of Poland's cybersecurity system, highlighting the difficulties in aligning national legislation with the dynamic requirements of the EU and the shortage of qualified personnel. Meanwhile, Chernysh et al.[11] examined Ukraine's critical infrastructure protection system, emphasising its unique development under conditions of continuous cyber aggression and the need to strengthen the military component of cyber defence.

Despite the considerable volume of research covering both general theoretical frameworks and narrowly specialised technical issues, a certain gap remains in the academic literature. There is a lack of comprehensive comparative legal analysis that systematically contrasts national approaches of countries with different legal traditions and geopolitical contexts (e.g., EU member states, a non-European federal state, and a country at war). Existing studies rarely combine dogmatic analysis of national legislation with reviews of international reports and academic literature to illustrate how national strategies respond to global technological and security trends. Thus, the issue of how differences in state governance and security environments influence the development of national models for the protection of critical information infrastructure remains insufficiently explored. The objective of this article is to conduct a comparative study of governmental approaches to securing critical information systems in order to identify commonalities and divergences in the legal and institutional models of Poland, the Netherlands, Ukraine, and Canada. To achieve this objective, the following tasks were defined: to analyse the legal and strategic documents of the selected countries; to compare their institutional mechanisms and approaches to risk management; and to align national models with key international standards and academic concepts in the field of cybersecurity.

10 M. Ojdana-Kościuszko, *Evolution and challenges of the Polish cybersecurity system*, in *On Security and Defence*, 2024, Vol. 10, No. 1, pp. 128-146.

11 R. Chernysh, M. Chekhovska, O. Stoliarenko, O. Lisovska, A. Lyseiuk, *Ensuring information security of critical infrastructure objects as a component to guarantee Ukraine's national security*, in *Amazonia Investiga*, 2023, Vol. 12, No. 67, pp. 87-95.

2. Materials and methods

This study was conducted during May-June 2025 and was of a theoretical and comparative-legal nature. For the purpose of carrying out the comparative analysis, four countries were selected: Poland, the Netherlands, Ukraine, and Canada. The selection of these jurisdictions was based on their substantial differences, which enabled the study to represent a diverse range of models for governmental cybersecurity governance. Specifically, Poland and the Netherlands were selected as representatives of the EU, allowing for an analysis of the implementation and national adaptation of common EU regulatory frameworks. Ukraine represents a unique case of a country developing its cybersecurity system in the context of full-scale warfare, rendering its experience valuable for assessing resilience and crisis management. Canada was included as an example of a large federal state with a common law tradition, enabling a comparison between its approach and continental European models, as well as an examination of the specificities of interaction between federal and provincial levels of government.

The empirical basis of the study included: supranational EU acts, notably Directive (EU) 2022/2555[12]; national legislation of Poland[13], the Netherlands[14], Ukraine[15], and Canada[16]. To contextualise and analyse international practices, analytical reports from leading organisations were used, including Accenture[17],

12 Directive (EU) 2022/2555 of the European Parliament and of the Council "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" (NIS2 Directive), 2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

13 Act of Poland "On the National Cybersecurity System," 2018. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560

14 Act of Netherland "On Network and Information Systems Security," 2018. https://www.digitaltrustcenter.nl/wet-beveiliging-netwerk-en-informatiesystemen-wbni

15 Law of Ukraine No. 45 "On the Basic Principles of Ensuring Cybersecurity of Ukraine," 2017. https://zakon.rada.gov.ua/laws/show/2163-19#Text; Cybersecurity strategy of Ukraine (2021-2025), 2021. https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

16 Telecommunications Act, 1993. https://laws.justice.gc.ca/eng/acts/t-3.4/; Bill C-26: An Act Respecting Cyber Security, amending the Telecommunications Act and making consequential amendments to other Acts, 2022. https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c26_1.html; Critical Cyber Systems Protection Act, 2025. https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20250226-1/07-en.aspx; Canada's National Cyber Security Strategy, 2025. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx

17 Accenture, "State of cybersecurity resilience 2025," 2025. https://www.accenture.com/content/dam/accenture/final/accenture-com/document-3/State-of-

CompTIA[18], the Organisation for Economic Co-operation and Development (OECD)[19], and Ukrainian think tanks[20]. Selected cases and events were analysed based on information bulletins[21].

The methodological framework of the research comprised general scientific and specialised legal methods. The dogmatic (formal-legal) method was employed to analyse the content of normative legal acts, interpret legal norms, determine the powers of public authorities and obligations of critical infrastructure operators. The comparative-legal method was key in contrasting the legal systems of the selected countries and identifying similarities and differences in their approaches to cybersecurity regulation. The system-structural method enabled the examination of national cybersecurity systems as integrated complexes of interconnected elements (institutions, norms, functions) and facilitated the analysis of their internal coherence. Additionally, the legal-hermeneutic method was used to interpret the content of strategic documents and legal concepts, particularly the Dutch principle of the "duty of care" (zorgplicht).

Cybersecurity-report.pdf

18 CompTIA, "State of cybersecurity," 2025. https://www.comptia.org/en-us/resources/research/state-of-cybersecurity/

19 Organisation for Economic Co-operation and Development, "Government at a glance 2025," 2025. https://www.oecd.org/en/publications/government-at-a-glance-2025_0efd0bcd-en.html

20 Annual Analytical Review, 2024. https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year in review_UKR_upd.pdf

21 Forbes Ukraine, "Cyberattack on Kyivstar will cost parent company Veon nearly $100 million," 2024. https://forbes.ua/news/kiberataka-na-kiivstar-obiydetsya-materinskiy-kompanii-veon-u-mayzhe-100-mln-18012024-18595; Ministry of Foreign Affairs of Ukraine, "One year of the Tallinn Mechanism: 200 million euros for the cybersecurity of Ukraine's civilian infrastructure," 2024. https://mfa.gov.ua/news/rik-roboti-tallinskogo-mehanizmu-200-miljoniv-yevro-dlya-kiberzahistu-civilnoyi-infrastrukturi-ukrayini; State Service of Special Communications and Information Protection of Ukraine, "Together in defending cyberspace: State Service of Special Communications, NCCC and ENISA signed a cooperation agreement," 2023. https://cip.gov.ua/ua/news/razom-na-zakhisti-kiberprostoru-derzhspeczv-yazku-nkck-ta-enisa-pidpisali-ugodu-pro-spivpracyu

3. Results

3.1. Legislative regulation and institutional framework for cybersecurity in the Republic of Poland

Poland's legal framework in the area of cybersecurity has been significantly shaped by pan-European initiatives, notably NIS2 Directive[22]. The foundational national document in this domain is the Act "On the National Cybersecurity System"[23]. This Act laid the foundation for the functioning of a comprehensive, multi-tiered system integrating state authorities, operators of essential services (operator zyusługklu czowych), and digital service providers in a joint effort to counter cyber threats. The necessity of such strict regulation stems from the global context: according to Accenture[24], 72% of organisations worldwide reported an increase in cyber threats, with 63% identifying the evolving threat landscape as their greatest challenge. A dogmatic analysis of the Act of Poland "On the National Cybersecurity System"[25] revealed that it is grounded in the principle of identifying and protecting entities whose operations are critical to the functioning of the state and society. Article 5 of the Act established clear criteria and procedures for identifying operators of essential services across sectors such as energy, transport, healthcare, banking, financial market infrastructure, and digital supply. The same article mandated competent authorities (sectoral ministries) to maintain registries of such operators, thus ensuring a systemic supervisory approach. Identified operators were assigned a range of specific obligations, detailed in Articles 8-10 of the Act "On the National Cybersecurity System"[26]. Article 8, in particular, required them to implement an adequate and proportionate information security management system covering both technical and organisational

22 Directive (EU) 2022/2555 of the European Parliament and of the Council "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" (NIS2 Directive), 2022.

23 Act of Poland "On the National Cybersecurity System," 2018. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560

24 Accenture, "State of cybersecurity resilience 2025," 2025. https://www.accenture.com/content/dam/accenture/final/accenture-com/document-3/State-of-Cybersecurity-report.pdf

25 Act of Poland "On the National Cybersecurity System," 2018.

26 *Ibid.*

aspects. This includes the development and implementation of internal security policies, systematic risk assessments, the creation of business continuity plans, and incident management procedures.

A crucial element introduced in Article 9 was the obligation to conduct audits of information systems used in the provision of essential services at least once every two years[27]. This approach responds to global challenges, as evidenced by the CompTIA[28], which found that 59% of North American companies experienced moderate or significant impacts from cyber incidents over the past year. Article 10 of the Act "On the National Cybersecurity System"[29] imposed the obligation to report "serious incidents" (incident poważny) to the Computer Security Incident Response Team (CSIRT) within 24 hours of detection. This provision aims to establish a nationwide threat picture and enable rapid systemic responses, which is particularly relevant given that only 28% of organisations, according to Accenture[30], implement security measures at the initial stage of transformation initiatives, often resulting in reactive rather than proactive threat responses.

The institutional structure defined in Article 20 of the Act of Poland "On the National Cybersecurity System"[31] is three-tiered. It includes a Government Plenipotentiary for Cybersecurity (typically at the ministerial or deputy ministerial level responsible for digital affairs), who performs a coordinating function at the political level. The technical level is represented by three national-level CSIRTs, whose mandates are outlined in Article 26[32]. These include: CSIRT GOV, operating within the Internal Security Agency and responsible for government institutions; CSIRT MON, tasked with the defence sector; and CSIRT Scientific and Academic Computer Network (NASK), serving operators of essential and digital services as well as other entities. This differentiation enables a specialised approach, which is crucial given that, according to the Accenture (2025), 90% of companies lack sufficient maturity to counter modern threats, in-

27 *Ibid.*
28 CompTIA, "State of cybersecurity," 2025.
29 Act of Poland "On the National Cybersecurity System," 2018.
30 *Ibid.*
31 Accenture, "State of cybersecurity resilience 2025," 2025.
32 Act of Poland "On the National Cybersecurity System," 2018.

cluding AI-driven ones. The Act of Poland "On the National Cybersecurity System"[33] also established a robust system of oversight and accountability detailed in Chapter 7.

Competent authorities (sectoral ministries) were granted powers to conduct scheduled and unscheduled inspections of essential service operators. In the event of violations, Article 62 of the Act "On the National Cybersecurity System"[34] authorised them to impose financial penalties, which may amount to significant sums (up to PLN 200,000 for individual breaches, and up to PLN 1,000,000 in cases of repeated non-compliance). This creates an effective incentive mechanism to ensure compliance with legal requirements. The need for such financial incentives is corroborated by data from State of Cybersecurity[35], which indicates that 36% of companies consider budget constraints the primary barrier to improving cybersecurity, as well as findings from the European Union Agency for Cybersecurity (ENISA) Annual Analytical Review[36], which reported that in 2022, 47% of critical infrastructure operators in the EU did not plan to hire new cybersecurity professionals. At the same time, according to the OECD[37], Poland's overall score for ex post legislative evaluation remains low (1.5 out of 4), indicating potential challenges in assessing the effectiveness of the Act "On the National Cybersecurity System"[38] itself.

In conclusion, the analysis of the Polish approach illustrates the formation of a classical European model focused on harmonisation and alignment with EU norms. This model is characterised by a high degree of formalisation, a clear distribution of institutional competences, and the presence of effective mechanisms of financial liability for operators. Nevertheless, the identified low quality of ex post legislative evaluation suggests a potential gap between formal compliance and the actual effectiveness of the system, posing a systemic challenge for similar regulatory regimes.

---

33 *Ibid.*

34 *Ibid.*

35 CompTIA, "State of cybersecurity," 2025.

36 Annual Analytical Review, 2024.

37 Organisation for Economic Co-operation and Development, "Government at a glance 2025," 2025.

38 Act of Poland "On the National Cybersecurity System," 2018.

3.2. The Dutch approach to harmonising national legislation with EU cybersecurity norms

The Netherlands, as one of the most digitalised OECD countries, has demonstrated a mature and flexible approach to the implementation of EU cybersecurity directives. The cornerstone of national legislation is the Act "On Network and Information Systems Security"[39], which entered into force on 9 November 2018, transposing NIS2 Directive[40]. A doctrinal analysis of this law reveals that the Dutch model, unlike the more formalised Polish approach, is characterised by a high degree of integration of cybersecurity into the broader crisis management system, a strong emphasis on public-private partnership, and a focus on sectoral specialisation. This model is supported by high levels of governance effectiveness; according to the OECD[41], the Netherlands ranks among the top performers in terms of public sector management quality and consistently enjoys high levels of public trust in governmental institutions, thereby creating favourable conditions for the implementation of complex regulatory policies.

The Act of Netherland "On Network and Information Systems Security"[42], similarly to its Polish counterpart, defines in Articles 2 and 3 the categories of "essential service providers" and "digital service providers". However, unlike a fixed list, the Dutch legislator established framework criteria that allow the government to flexibly determine and update the list of entities through subordinate legislation. The key obligations of operators are articulated through two central legal concepts: the "duty of care" (zorgplicht) and the "duty to notify" (meldplicht). The principle of zorgplicht is less prescriptive than its Polish equivalent; it requires operators to take all "appropriate and proportionate technical and organisational measures" to manage risks and prevent incidents[43]. This encourages self-assessment of risks rather than mere compliance with formal requi-

39 Act of Netherland "On Network and Information Systems Security," 2018.

40 Directive (EU) 2022/2555 of the European Parliament and of the Council "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" (NIS2 Directive), 2022.

41 Organisation for Economic Co-operation and Development, "Government at a glance 2025," 2025.

42 Act of Netherland "On Network and Information Systems Security," 2018.

43 *Ibid.*

rements, which is crucial in the context where, as noted by CompTIA[44], 44% of organisations face a wide variety of attack vectors. The meldplicht principle obliges operators to notify the National Cyber Security Centre (NCSC) and the relevant supervisory authority "without undue delay" of incidents that have "significant consequences" for service provision.

The institutional architecture of the Netherlands is centralised in coordination yet decentralised in supervision. The NCSC plays a pivotal role as a centre of expertise, information exchange, and national-scale incident response[45]. Meanwhile, supervisory functions (toezicht) are assigned to sectoral ministries and specialised regulators such as the Telecommunications Agency (Agentschap Telecom) for digital infrastructure or the Health and Youth Care Inspectorate (Inspectie Gezondheidszorgen Jeugd). This approach enables sector-specific risk consideration, a critical prerequisite for effective protection, as evidenced by the Annual Analytical Review[46], which highlights the increasing intensity of attacks on operational technologies (OT), requiring in-depth sectoral expertise. The NCSC actively cooperates with the private sector through the National Cyber Incident Response Forum (NIRF), exemplifying a successful public-private partnership model. The effectiveness of such collaboration is underscored in the Accenture[47], which states that organisations in the "Reinvention-Ready Zone" exhibit significantly higher levels of security integration into business strategy.

A distinctive feature of the Dutch approach is its strong focus on data protection, which gained particular relevance following the leak of personal data of all Dutch police officers in September 2023[48]. This incident prompted a national reassessment of security policies and confirmed the Accenture (2025) regarding the existence of a "Security Maturity Gap", as 77% of organisations reportedly lack basic data and artificial intelligence (AI) security practices. In response, the

---

44 CompTIA, "State of cybersecurity," 2025.

45 M. GULIYEV, H. MURADOVA, L. HAJIYEVA, L. HUSEYNOVA, *Comparative analysis of marketing strategies of global corporations in industrial and innovation clusters in Europe and China*, in *Strategic Change*, 2025, Vol. 34, No. 5, pp. 689–701; S. PORKODI, A. M. RAMAN, *Success of cloud computing adoption over an era in human resource management systems: A comprehensive meta-analytic literature review*, in *Management Review Quarterly*, 2025, Vol. 75, No. 2, pp. 1041–1075.

46 Annual Analytical Review, 2024.

47 Accenture, "State of cybersecurity resilience 2025," 2025.

48 Annual Analytical Review, 2024.

Dutch government strengthened personal data protection requirements and access control mechanisms in public information systems. Furthermore, the reality of threats was corroborated by the Dutch military intelligence report, which in 2024 uncovered a large-scale cyberespionage campaign conducted by China. This campaign had remained undetected for an extended period and enabled attackers to penetrate the country's military networks[49]. This incident demonstrates that even the most technologically advanced states remain vulnerable to sophisticated state-sponsored cyberattacks, justifying the need for continuous enhancement of national cybersecurity systems.

3.3. Ukraine's experience in developing a cybersecurity system under martial law

Ukraine represents a unique case of a state building its national cybersecurity system amidst a protracted cyberwar that began in 2014 and escalated into full-scale conflict on 24 February 2022[50]. This context has profoundly influenced legislative priorities, regulatory frameworks, and institutional architecture, compelling the state to transition rapidly from theoretical frameworks to practical measures within highly compressed timeframes. Foundational documents in this domain include the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine"[51] and the Cybersecurity Strategy of Ukraine (2021-2025)[52]. Developed prior to the full-scale invasion, these instruments laid the groundwork that proved critical to organising resistance in cyberspace.

A doctrinal analysis of the Law "On the Basic Principles of Ensuring Cybersecurity of Ukraine"[53] shows that it established key terminology and institutional parameters. Article 1 defines terms such as "cybersecurity", "cyberattack", "cyber incident", and "critical information infrastructure objects", thereby creating a unified terminological foundation. The institutional system outlined in Articles 8-12 is multi-actor. The National Coordination Centre for Cyberse-

49 *Ibid.*

50 *Ibid.*

51 Law of Ukraine No. 45 "On the Basic Principles of Ensuring Cybersecurity of Ukraine," 2017.

52 Cybersecurity strategy of Ukraine (2021-2025), 2021.

53 Law of Ukraine No. 45 "On the Basic Principles of Ensuring Cybersecurity of Ukraine," 2017.

curity (NCCC) under the National Security and Defence Council of Ukraine plays the coordinating role. Pursuant to Article 11 of the Law, the NCCC analyses the cybersecurity situation and coordinates the activities of security and defence sector entities. The State Service of Special Communications and Information Protection of Ukraine (SSSCIP)[54], under Article 9, is the principal body responsible for cyber protection of state information resources and critical infrastructure and operates the national computer emergency response team Computer Emergency Response Team of Ukraine (CERT-UA). The Security Service of Ukraine (SSU), according to Article 10, focuses on counterintelligence, combating cyberterrorism, and cyberespionage.

The Cybersecurity Strategy of Ukraine[55], adopted six months before the full-scale invasion, has proven highly prescient and is based on three core principles: deterrence, cyber resilience, and cooperation. Under wartime conditions, the priority of "deterrence" has gained exceptional importance. Strategic Goal S.1 "Effective Cyber Defence" directly envisaged the creation of a separate branch of the Armed Forces of Ukraine–the Cyber Defence Forces – reflecting the global trend of cyber domain militarisation[56]. This goal was realised in direct response to the Russian Federation's aggressive actions. Moreover, Goal S.2 aims to strengthen capabilities to counter intelligence and subversive activities, which remains a daily reality for Ukraine. The Annual Analytical Review[57] notes that attacks on military personnel aimed at stealing intelligence remain a strategic objective of the adversary.

The large-scale cyberattack on the national mobile operator Kyivstar in December 2023 was a major incident that starkly demonstrated the vulnerabilities of critical infrastructure[58]. The attack caused a network outage lasting several days, with full-service restoration taking several weeks. According to the SSU, Russian hackers had planned a second wave of attacks intended to inflict even

54 State Service of Special Communications and Information Protection of Ukraine, "Together in defending cyberspace: State Service of Special Communications, NCCC and ENISA signed a cooperation agreement," 2023.

55 Cybersecurity strategy of Ukraine (2021-2025), 2021.

56 *Ibid.*

57 Annual Analytical Review, 2024.

58 Forbes Ukraine, "Cyberattack on Kyivstar will cost parent company Veon nearly $100 million," 2024.

greater damage[59]. This incident confirmed that even with significant international support, critical infrastructure remains at exceptionally high risk. In January 2024, new powerful attacks targeted the banking sector and one of Ukraine's largest data centres, causing temporary disruptions to numerous public services. According to CERT-UA, 2024 saw increased adversary interest in Ukraine's telecommunications sector, alongside widespread use of phishing campaigns via messaging apps disguised as military-related documents[60].

In response to these threats, Ukraine is actively enhancing its own capabilities in line with Objective C.1 "Strengthening national cyber readiness and cybersecurity"[61]. According to the Annual Analytical Review[62], the National Cybersecurity Coordination Centre (NCCC) conducted the HackWave and INCIDENT RESPONSE DAYS 2.0 cybersecurity competitions, as well as the first sectoral exercises for the transport sector – CIREX.CoBridge. To raise public awareness, the Ministry of Digital Transformation launched the "Cybergram" test, and the SSSCIP held a nationwide online cybersecurity lesson attended by over 20,000 viewers. The first national cyber range, Cyber Range UA, aimed at the practical training of specialists, was presented at the National Aviation University[63]. Ukraine's experience has demonstrated the critical importance of international cooperation, reflected in Objective B.3 "Pragmatic international cooperation" of the Cybersecurity Strategy of Ukraine[64].

In December 2023, Estonia and nine other countries launched the Tallinn Mechanism to systematise civilian cyber assistance to Ukraine[65]. In November 2023, a Cooperation Agreement was signed with ENISA[66], marking the first such document between the European agency and a non-EU country. Additionally, Denmark announced the provision of USD 13 million in cyber assistance, and

59 Annual Analytical Review, 2024.

60 Annual Analytical Review, 2024.

61 Cybersecurity strategy of Ukraine (2021-2025), 2021.

62 Annual Analytical Review, 2024.

63 *Ibid.*

64 Cybersecurity strategy of Ukraine (2021-2025), 2021.

65 Ministry of Foreign Affairs of Ukraine, "One year of the Tallinn Mechanism: 200 million euros for the cybersecurity of Ukraine's civilian infrastructure," 2024.

66 State Service of Special Communications and Information Protection of Ukraine, "Together in defending cyberspace: State Service of Special Communications, NCCC and ENISA signed a cooperation agreement," 2023.

the United States Agency for International Development (USAID) is assisting in enhancing cybersecurity in the energy sector[67]. The active involvement of Ukrainian law enforcement in international operations – particularly in dismantling the LockBit and IcedID infrastructures under Operation Endgame – demonstrates their high level of competence. In June 2024, it was reported that prosecutors of the International Criminal Court (ICC) were investigating Russian cyberattacks on Ukraine's civilian infrastructure as war crimes, while the SSU is gathering evidence concerning the attack on Kyivstar for submission to the ICC[68]. This establishes an important precedent for accountability for cybercrimes at the international level.

3.4. Strategic priorities and federal – Provincial interaction in Canada's cybersecurity system

Canada's model for protecting critical information infrastructure differs significantly from European approaches due to its federal structure and the absence of a supranational regulator. The system is based on Canada's National Cyber Security Strategy[69], updated in 2024, and new legislative instruments, in particular Bill C-26[70], which amended the Telecommunications Act[71] and introduced the Critical Cyber Systems Protection Act (CCSPA)[72]. An analysis of these documents reveals that Canada's key priorities are resilience, innovation, and collaboration, implemented through a multi-level governance model. The OECD[73] noted that in federal states like Canada, a significant share of regulatory and service delivery responsibilities lies with subnational entities. Data from 2023 indicate that 51% of public investment in Canada occurred at the provincial level, compared to only 11% at the federal level.

67 Annual Analytical Review, 2024.

68 *Ibid*.

69 Canada's National Cyber Security Strategy, 2025.

70 Bill C-26: An Act Respecting Cyber Security, amending the Telecommunications Act and making consequential amendments to other Acts, 2022.

71 Telecommunications Act, 1993.

72 Critical Cyber Systems Protection Act, 2025.

73 Organisation for Economic Co-operation and Development, "Government at a glance 2025," 2025.

This division of powers is also reflected in the cybersecurity system[74]. While the federal Canadian Centre for Cyber Security (CCCS) functions as the central authority on cyber protection, substantial responsibility for practical policy implementation rests with provincial governments and critical infrastructure operators. The national strategy explicitly emphasises the need for close coordination across all levels of government, aligning with the findings of the CompTIA report[75], which showed that 39% of companies identified a disconnect between cybersecurity policy and business operations. The new CCSPA[76] targets federally regulated operators in key sectors – telecommunications, energy, transport, and finance – and mandates the development and implementation of comprehensive cybersecurity programmes. These programmes must include risk detection and management measures, particularly those related to supply chains and third parties. Operators are also obliged to report cyber incidents immediately to the CCCS. A significant innovation of the Act is the granting of authority to the Government of Canada to issue binding cybersecurity directions for the protection of critical systems in the event of significant threats[77].

The Canadian strategy identifies ten critical infrastructure sectors and places a strong emphasis on innovation and workforce development, responding to the global shortage of qualified professionals. According to the Accenture report[78], 83% of executives consider the talent gap the main obstacle to maintaining adequate security levels. To address this, the Canadian strategy includes investments in educational programmes and initiatives to train the next generation of professionals. Another vital element is the "Cyber Secure Canada" programme – a voluntary certification for small and medium-sized enterprises (SMEs) to help implement baseline cybersecurity standards. This initiative aims to streng-

74 A. DALKE, S. SVYATOV, E. RUZIYEVA, *Criteria for identification and regulation of systemically important banks*, in *Accounting, Economics and Law: A Convivium*, 2025. https://doi.org/10.1515/ael-2024-0070

75 CompTIA, "State of cybersecurity," 2025.

76 Critical Cyber Systems Protection Act, 2025.

77 A. BARLYBAYEV, A. TURGINBAYEVA, *Development and implementation of an advanced fuzzy expert system for the assessment of information security risks*, in *Journal of Computational and Cognitive Engineering*, 2025, Vol. 4, No. 4, pp. 570–580; A. BARLYBAYEV, A. SHARIPBAY, G. Shakhmetova, A. ZHUMADILLAYEVA, *Development of a flexible information security risk model using machine learning methods and ontologies*, in *Applied Sciences*, 2024, Vol. 14, No. 21, p. 9858.

78 Accenture, "State of cybersecurity resilience 2025," 2025.

then supply chain resilience, as reports indicate that SMEs often represent a weak link in the cybersecurity ecosystem[79]. Canada's participation in international alliances, notably the "Five Eyes," ensures access to intelligence and best practices[80]. Joint guidance on the Volt Typhoon threat actor, issued together with the United States, Australia, New Zealand, and the United Kingdom, serves as an example of such collaboration[81].

Thus, the analysis of Canada's approach reveals the emergence of a unique federal model that significantly differs from the unitary systems of Europe. It is characterised by the combination of three key elements: clear legislative regulation at the federal level for critical sectors; encouragement of voluntary initiatives to enhance private sector resilience; and the prioritisation of international cooperation within intelligence-sharing alliances. This comprehensive approach reflects Canada's commitment to balancing centralised strategic leadership with flexibility and broad stakeholder engagement.

3.5. Comparative analysis and summary of findings

The conducted study of national approaches to the protection of critical information infrastructure in Poland, the Netherlands, Ukraine, and Canada revealed both common trends – driven by the global nature of cyber threats – and significant differences, which reflect the unique legal, political, and security contexts of each country. A shared feature among all jurisdictions examined is the recognition of cybersecurity of critical infrastructure as a key national security priority and the shift towards proactive risk management, rather than mere incident response[82]. This shift is confirmed by report data indicating an exponential increase in the number and complexity of cyberattacks, prompting governments

79 *Ibid*.

80 Annual Analytical Review, 2024.

81 Ibid; T. Feng, H. Pei, Z. Jin, X. Wu, *A survey and perspective on electronic design automation tools for ensuring SoC security*, in *19th International SoC Design Conference*, Institute of Electrical and Electronics Engineers, 2022, pp. 215-216; F. A. F. Alazzam, H. J. M. Shakhatreh, Z. I. Y. Gharaibeh, I. Didiuk, O. Sylkin, *Developing an information model for e-commerce platforms: A study on modern socio-economic systems in the context of global digitalization and legal compliance*, in *Information Systems Engineering*, 2023, Vol. 28, No. 4, pp. 969-974.

82 B. R. Rexhepi, A. Kumar, M. S. Gowtham, R. Rajalakshmi, M. D. Paikaray, P. K. Adhikari, *A secured intrusion detection system integrated with the conditional random field for the MANET network*, in *International Journal of Intelligent Systems and Applications in Engineering*, 2023, Vol. 11, No. 3s, pp. 14–21.

to strengthen regulatory requirements[83]. Differences in approaches, shaped by national priorities and legal traditions, become particularly evident in the analysis of strategic frameworks and practical mechanisms for policy implementation (Table 1).

Table 1. Comparison of strategic approaches and implementation mechanisms

Approach	Poland	Netherlands	Ukraine	Canada
Primary focus of the strategy	Compliance with EU norms, building a national system based on the NIS2 model	Proactive risk management, public-private partnerships, data protection	Cyber defence, deterring aggressors, resilience in wartime conditions	Critical infrastructure resilience, innovation, federal-provincial collaboration
Role of the state	Regulator and supervisory authority	Coordinator and partner	Commander and defender	Facilitator and strategic partner
Public-private partnership model	Mandatory reporting and compliance through CSIRT NASK	Joint platforms for information exchange (NCSC, NIRF)	Engagement of cyber volunteers, contractual basis for IT Army	Voluntary certification ("Cyber Secure"), joint working groups
Approach to cyber incidents	Centralised reporting via specialised CSIRTs	Centralised reporting and coordination through NCSC	Multi-level response (military, law enforcement, technical)	Decentralised reporting with coordination via CCCS
Priorities in international cooperation	Participation in EU programmes (ENISA, Permanent Structured Cooperation – PESCO) and North Atlantic Treaty Organisation (NATO)	Active role in ENISA, Europol, bilateral agreements	Cooperation with NATO, EU (ENISA), US, Tallinn Mechanism	Participation in the Five Eyes alliance, bilateral agreements with the US
Approach	Adaptation to NIS2	Development	Training	Youth engagement

83 Accenture, "State of cybersecurity resilience 2025," 2025; CompTIA, "State of cybersecurity," 2025.

to workforce developme nt	requirements, upskilling civil servants	of specialised skills, training programmes for public officials	military cyber specialists, development of cyber ranges	programmes, addressing workforce shortages in the public sector

[Source: compiled by the authors based on Annual Analytical Review[84]; Accenture[85]; CompTIA[86]]

A comparative legal analysis has identified three distinct models of state regulation. Poland and the Netherlands represent a European harmonised model, grounded in the implementation of the NIS2 Directive[87]. This model is characterised by the clear designation of operators of essential services, the establishment of specific risk management and reporting obligations, and the creation of a network of national competent authorities and CSIRTs. Despite sharing a common legal framework, philosophical divergences were observed: Polish legislation[88] is more prescriptive, setting out detailed timelines and procedures, whereas Dutch law[89] emphasises the "duty of care" (zorgplicht) principle, offering operators greater flexibility in selecting security measures.

Ukraine presents a model of resilience under conditions of war. Its approach is militarised and crisis-oriented, driven by the need to counter continuous large-scale cyber aggression. This is reflected in the strategic objective of establishing military cyber forces[90], active counterintelligence operations, and the prioritisation of critical infrastructure protection as a component of national defence[91]. The Ukrainian model also demonstrates a unique degree of societal mobilisation and unprecedented depth of international cooperation, extending beyond

84 Annual Analytical Review, 2024.

85 Accenture, "State of cybersecurity resilience 2025," 2025; CompTIA, "State of cybersecurity," 2025.

86 CompTIA, "State of cybersecurity," 2025.

87 Directive (EU) 2022/2555 of the European Parliament and of the Council "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" (NIS2 Directive), 2022.

88 Act of Poland "On the National Cybersecurity System," 2018.

89 Act of Netherland "On Network and Information Systems Security," 2018.

90 Cybersecurity strategy of Ukraine (2021-2025), 2021.

91 O. KHODAKIVSKA, M. MARTYNIUK, Y. LUPENKO, *Prospective analysis of the implementation of the "green" economy in the agricultural sector of Ukraine for the next 10 years*, in *Scientific Horizons*, 2023, Vol. 26, No. 10, pp. 163–179.

standard information sharing to include direct technical assistance, such as the Tallinn Mechanism[92] and the IT Coalition[93], as well as the investigation of cyberattacks as war crimes by the ICC[94].

Canada implements a federal partnership-based model. This approach stems from its state structure, wherein significant powers are vested in the provinces, as corroborated by OECD[95] on decentralised public investment. Canada's strategy and legislation[96] emphasise collaboration between the federal government, provincial authorities, and the private sector. The main instruments include not only mandatory requirements for operators in federally regulated sectors but also voluntary programmes such as Cyber Secure Canada, and an extensive information-sharing network facilitated by the CCCS. Canada's international cooperation is largely conducted within the Five Eyes alliance, which focuses on intelligence sharing[97].

Thus, the study concludes that state approaches to securing critical information systems are evolving from strictly technical mechanisms to comprehensive socio-legal systems. In the EU, this process is driven by the imperative of internal market harmonisation; in Ukraine, by an imminent military threat; and in Canada, by the necessity for coordination within a complex federal state. All countries face shared challenges such as workforce shortages and supply chain protection, compelling them to seek a balance between regulation, incentivisation, and international cooperation[98]. For the purpose of systematisation and vi-

92 Ministry of Foreign Affairs of Ukraine, "One year of the Tallinn Mechanism: 200 million euros for the cybersecurity of Ukraine's civilian infrastructure," 2024.

93 State Service of Special Communications and Information Protection of Ukraine, "Together in defending cyberspace: State Service of Special Communications, NCCC and ENISA signed a cooperation agreement," 2023.

94 Annual Analytical Review, 2024.

95 Organisation for Economic Co-operation and Development, "Government at a glance 2025," 2025.

96 Critical Cyber Systems Protection Act, 2025.

97 Annual Analytical Review, 2024.

98 Accenture, "State of cybersecurity resilience 2025," 2025; CompTIA, "State of cybersecurity," 2025; B. M. NURGALIEV, K. S. LAKBAYEV, A. V. BORETSKY, A. K. KUSSAINOVA, *The informal funds transfer system "hawala" as a segment of the shadow economy: Social impact assessment and framework for combating*, in *American Journal of Applied Sciences*, 2015, Vol. 12, No. 12, pp. 931–937; B. M. NURGALIEV, K. S. LAKBAYEV, A. K. KUSSAINOVA, A. V. BORETSKY, *Impact of organized crime on shadow economy: Social impact assessment*, in *Asian Journal of Applied Sciences*, 2014, Vol. 7, No. 1, pp. 644–651.

sual comparison of the key legal regulatory elements in the examined countries, the core provisions of their legislative and institutional frameworks have been consolidated in Comparative Table 2.

Table 2. Comparative analysis of legislative and institutional cybersecurity frameworks

Criterion	Poland	Netherlands	Ukraine	Canada
Key legislative act	Act "On the National Cybersecurity System"[99]	Act "On Network and Information Systems Security"[100]	Law "On the Basic Principles of Ensuring Cybersecurity of Ukraine"[101]	Critical Cyber Systems Protection Act[102]
Implementation of EU norms	Direct transposition of the NIS Directive; ongoing adaptation to NIS2	Direct transposition of the NIS Directive; ongoing adaptation to NIS2	Active harmonisation with NIS2 norms within European integration	Not applicable (domestic model)
Key coordinating body	Government Plenipotentiary for Cybersecurity	NCSC	NCCC	CCCS
Primary supervisory entities	Sectoral ministries	Sectoral ministries and specialised regulators (e.g., Telecommunications Agency)	SSSCIP, Security Service of Ukraine (SBU), National Police, National Bank of Ukraine (NBU)	Federal regulators for respective sectors

99 Act of Poland "On the National Cybersecurity System," 2018.

100 Act of Netherland "On Network and Information Systems Security," 2018.

101 Law of Ukraine No. 45 "On the Basic Principles of Ensuring Cybersecurity of Ukraine," 2017.

102 Critical Cyber Systems Protection Act, 2025.

Definition of critical infrastructure	Operators of essential services	Providers of essential services	Critical information infrastructure facilites (CIIF)	Operators of vital services/systems
Key operator obligations	Risk assessment, implementation of security measures, auditing, incident reporting	"Duty of care" and "duty to report"	Implementation of comprehensive protection systems, auditing, incident reporting	Development of cybersecurity programmes, risk management, reporting, compliance with government directives
Sanctions mechanism	Administrative (financial penalties up to 1 million PLN)	Administrative (financial penalties)	Administrative and criminal liability	Administrative fines and regulatory measures

[Source: compiled by the authors based on Annual Analytical Review[103]; Organisation for Economic Co-operation and Development[104]]

The systematised comparative analysis of the legislative and institutional frameworks clearly illustrates the divergences among the identified models. On one hand, the European approach (Poland, Netherlands) is marked by the direct implementation of common EU norms and the establishment of a clear hierarchy of regulators and supervisory bodies. On the other hand, the Ukrainian and Canadian models are outcomes of unique national circumstances. Ukraine's wartime system exhibits a distinctly militarised character, involving security agencies (SBU, State Service for Special Communications) in supervisory roles and criminal liability for violations[105]. The Canadian model, by contrast, reflects its federal structure, where the CCCS functions as the central coordinating body alongside federal regulators, and the sanction mechanism includes not only fines but also regulatory actions. Hence, the analysis affirms that despite facing common threats, legal and institutional responses remain profoundly dependent on

103 Annual Analytical Review, 2024.

104 Organisation for Economic Co-operation and Development, "Government at a glance 2025," 2025.

105 S.-C. KIM, J.-K. CHUNG, N. TRUSOVA, Z. AKHMETOVA, N. MUSAYEVA, *Simulating global supply chain reverberations from Ukrainian grain shipment interruptions*, in *Revista Iberoamericana de Viticultura Agroindustria y Ruralidad*, 2025, Vol. 12, No. 34, pp. 192–207.

the national context, laying the groundwork for further discussion of each model's advantages and limitations.

4. Discussion

The comparative study of state approaches to the protection of critical information systems has revealed the emergence of three clearly delineated models: the European harmonised model (Poland, Netherlands), the Ukrainian wartime resilience model, and the Canadian federal partnership-based model. The results demonstrate that, despite shared global threats, national regulatory and institutional frameworks are deeply influenced by their respective political, historical, and security contexts. Correlating the data with scholarly findings allows not only to ascertain these differences but also to understand their implications and identify potential directions for the further improvement of national policies. A key conclusion from the results is that all countries under study consider cybersecurity a strategic priority requiring systemic state intervention. This aligns with the framework articulated by Pearlson et al.[106], who argued that information systems governance must be an integral part of both overall business strategy and organisational management. In this context, national cybersecurity laws can be seen as state-level attempts to strategically shape the environment in which critical infrastructure operators are compelled to integrate cybersecurity into their internal organisational strategies.

Findings show that Poland and the Netherlands are progressing towards the standardisation of requirements based on EU directives. This is consistent with Alexei[107], who demonstrated through the example of Moldova that the implementation of international standards such as International Standards Organisation (ISO) 27001 not only enhances the security posture of government entities but also strengthens trust among international partners by ensuring data confidentiality and integrity. Thus, the choice of Poland and the Netherlands in favour of the harmonised model can be interpreted not only as compliance with EU obligations but also as a pragmatic move towards increased investment attrac-

106 K. E. Pearlson, C. S. Saunders, D.F. Galletta, *Managing and using information systems: A strategic approach*, John Wiley & Sons, 2024.

107 A. Alexei, E*nsuring information security in public organizations in the Republic of Moldova through the ISO 27001 standard*, in *Journal of Social Sciences*, 2021, Vol. 4, No. 1, pp. 84-94.

tiveness and reliability in international relations. Meanwhile, the Ukrainian experience – analysed in detail by Khimko[108] in the context of cloud security standardisation – demonstrated that in a hybrid warfare environment, the drive towards international standards must be coupled with the development of unique national protocols tailored to counter threats specific to an aggressor state.

The study revealed that national legislation imposes high-level requirements on operators: conducting risk assessments, implementing security measures, and reporting incidents. However, a gap persists between legislative adoption and effective implementation, which can only be bridged through advanced technological solutions[109]. The study by Inaganti et al.[110] on Cloud Security Posture Management (CSPM) using AI illustrates how automation can facilitate monitoring, vulnerability detection, and regulatory compliance, aligning directly with the responsibilities placed on operators in Poland and the Netherlands. Without such AI-enhanced CSPM systems, compliance with the NIS2 Directive would be unfeasible for large-scale organisations. Similarly, the work by Mohammed[111] on Security Operations Centre (SOC) audits underscored the importance of continuous monitoring and log analysis for threat detection. This serves as a practical tool for fulfilling incident management obligations, enshrined in all four jurisdictions examined.

The fundamental objective of the national cybersecurity strategies analysed is the protection of core principles of information security, which, as defined by Yee and Zolkipli[112], comprise the CIA triad: Confidentiality, Integrity, and Availability. The legal obligations imposed on operators in Poland, the Netherlands, Ukraine, and Canada are essentially high-level mandates to implement

---

108 Ya. P. Khimko, *Standardisation of information security of cloud services*, in *Uzhhorod National University Herald. Series: Law*, 2025, Vol. 3, No. 88, pp. 61-66.

109 A. MUKANOV, A. SADUOV, Y. AKBAYEV, Z. DULATBEKOVA, A. OSPANOVA, I. SELEZNEVA, E. MADIYAROVA, G. JEMPEISSOVA, *Composing of scenarios development in strategic planning*, in *Journal of Environmental Management and Tourism*, 2018, Vol. 9, No. 3, pp. 491–500.

110 A. C. Inaganti, N. Ravichandran, S. R. K. Nersu, R. Muppalaneni, *Cloud security posture management (CSPM) with AI: Automating compliance and threat detection*, in *Artificial Intelligence and Machine Learning Review*, 2021, Vol. 2, No. 4, pp. 8-18.

111 A. Mohammed, *SOC audits in action: Best practices for strengthening threat detection and ensuring compliance*, in *Baltic Journal of Engineering and Technology*, 2023, Vol. 2, No. 1, pp. 62-69.

112 C. K. Yee, M. F. Zolkipli, *Review on confidentiality, integrity and availability in information security*, in *Journal of ICT in Education*, 2021, Vol. 8, No. 2, pp. 34-42.

controls that guarantee these principles. In this regard, Duggineni[113] emphasised that integrity control is critical to the operation of any information system, as it ensures the reliability and accuracy of data, which is essential for decision-making within critical infrastructure. In response to the growing complexity of modern systems, scholars propose cutting-edge technological solutions. Zubaydi et al.[114] and Faccia and Petratos[115] argued that blockchain technology holds significant potential for ensuring security and privacy within IoT ecosystems, and for integration with Enterprise Resource Planning (ERP) systems to create immutable and transparent records of transactions. For Industrial IoT (IIoT) systems, Hassan et al.[116] demonstrated the necessity of even more specialised approaches, including automated vulnerability detection and firmware hardening, which exceed general legal requirements. The Indonesian experience, where Putro et al.[117] developed a dedicated framework for critical infrastructure protection in the context of a "smart government", confirms this study's conclusion that each country must adapt global standards to its unique context. All of this unfolds against a backdrop of global trends, as described by Ghelani[118] and Desyatnyuk et al.[119], which highlight how rapid digitalisation, particularly in the financial sector, continuously generates new threat vectors, making the development and adaptation of national cybersecurity strategies an ongoing and essential process.

---

113 S. Duggineni, *Impact of controls on data integrity and information systems,* in *Science and Technology*, 2023, Vol. 13, No. 2, pp. 29-35.

114 H. D. Zubaydi, P. Varga, S. Molnár, *Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: A systematic literature review,* in *Sensors*, 2023, Vol. 23, No. 2, p. 788.

115 A. Faccia, P. Petratos, *Blockchain, enterprise resource planning (ERP) and accounting information systems (AIS): Research on e-procurement and system integration*, in *Applied Sciences*, 2021, Vol. 11, No. 15, p. 6792.

116 Y. G. Hassan, A. Collins, G. O. Babatunde, A. A. Alabi, S. D. Mustapha, *Automated vulnerability detection and firmware hardening for industrial IoT devices*, in *International Journal of Multidisciplinary Research and Growth Evaluation*, 2023, Vol. 4, No. 1, pp. 697-703.

117 P. A. W. Putro, D. I. Sensuse, W. S. S. Wibowo, *Framework for critical information infrastructure protection in smart government: A case study in Indonesia*, in *Information & Computer Security*, 2024, Vol. 32, No. 1, pp. 112-129.

118 D. Ghelani, *Cyber security, cyber threats, implications and future perspectives: A Review*, in *American Journal of Science, Engineering and Technology*, 2022, Vol. 3, No. 6, pp. 12-19.

119 O. Desyatnyuk, M. Naumenko, I. Lytovchenko, O. Beketov, *Impact of digitalization on international financial security in conditions of sustainable development*, in *Problems of Ecological Development*, 2024, Vol. 19, No. 1, pp. 104-114.

Particular attention in the course of this study was given to threats associated with the IoT and OT, which constitute the backbone of modern critical infrastructure, particularly smart grids. The findings of this research demonstrated that all countries recognise these sectors as priority areas for protection. The academic works of Tariq et al.[120] and Hasan et al.[121] provide in-depth technical insights into the understanding of these threats. Tariq et al.[122] emphasised that the IoT ecosystem is inherently vulnerable due to issues related to communication and management protocols. Hasan et al.[123] conducted a detailed analysis of the cyber-physical architecture of smart grids, identifying vulnerabilities in Supervisory Control and Data Acquisition (SCADA) and Advanced Metering Infrastructure (AMI) systems. These studies illustrate that the general legislative requirements identified in the course of this research are a necessary but insufficient condition for ensuring security. Specific technical standards and protocols are required, as discussed in the work of Tiwari et al.[124] concerning IoT security in the 5G era. Thus, a certain contradiction arises: while legislation establishes universal rules for all sectors, technological reality demands narrowly specialised solutions.

The Canadian model of sectoral resilience planning and the Dutch model of sectoral oversight represent attempts to reconcile this contradiction, aligning with the recommendations of the aforementioned authors. Supply chain security was identified as one of the key priorities in Canada's strategic documents and as one of the main threats in reports analysed by Ukrainian experts[125]. This fully corresponds with the conclusions of the scientific community. The study by

120 U. Tariq, I. Ahmed, A. K. Bashir, K. Shaukat, *A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review*, in *Sensors*, 2023, Vol. 23, No. 8, p. 4117.

121 M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, M. A. Razzaque, *Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations*, in *Journal of Network and Computer Applications*, 2023, Vol. 209, article no. 103540.

122 U. Tariq, I. Ahmed, A. K. Bashir, K. Shaukat, *A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review*, 2023.

123 M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, M. A. Razzaque, *Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations*, 2023.

124 P. Tiwari, N. Sharma, S. Chudhary, V. Gahlaut, *Ensuring IoT security in 5G era: Examining protocols, architectures, and security measures*, in A. Katti, R.K. Chourasia (Eds.), *Advances in Photonics and Electronics*, Cham: Springer. 2024, pp. 135-145.

Gangadhara[126] proposed the use of distributed ledger technology (blockchain) to ensure traceability and authentication of IIoT devices within supply chains. The national laws analysed in this study generally do not regulate security at the chip level, thereby creating a potential gap. This suggests that future state strategies will need to integrate not only software but also hardware aspects of cybersecurity, which will require even closer cooperation between legislators, regulators, and semiconductor manufacturers.

Finally, the results obtained allow for a re-examination of the relationship between cybersecurity and broader societal goals. The work of Ige et al.[127] proposed approaching cybersecurity strategies through the lens of the Sustainable Development Goals (SDGs). The conclusions of this study support this approach. Ensuring the resilience of energy, transport, and medical infrastructure (as demonstrated by the analysis across all four countries) directly contributes to the achievement of SDG 7 (Affordable and Clean Energy), SDG 9 (Industry, Innovation and Infrastructure), and SDG 3 (Good Health and Well-being)[128]. This is especially evident in the Ukrainian context, where the struggle for cyber resilience equates to the struggle to preserve the basic functions of the state and society, which is a fundamental prerequisite for any form of sustainable development. Moreover, the study by Mohammed[129] on cybersecurity in smart cities illustrates

125 S. Legominova, H. Haidur, *Analysis of modern threats to information security of organizations and the formation of an information platform to counter them,* in *Cybersecurity: Education, Science, Technique*, 2023, Vol. 2, No. 22, pp. 54-67.

126 B. Gangadhara, *Origin distributed ledger for ensuring it security in cloud manufacturing* in *International Journal of Multidisciplinary Engineering in Current Research*, 2021, Vol. 6, No. 7, pp. 27-40.

127 A. B. Ige, E. Kupa, O. Ilori, *Aligning sustainable development goals with cybersecurity strategies: Ensuring a secure and sustainable future,* in *GSC Advanced Research and Reviews*, 2024, Vol. 19, No. 3, pp. 344-360.

128 M. Guliyev, S. Rustamova, V. Makhmudova, T. Azizov, O. Huseynli, *The modern status and prospects for further development in the Australian energy sector: Transformation, external economic relations, investment climate*, in *Polityka Energetyczna*, 2023, Vol. 26, No. 3, pp. 47–64; L. Galchynskyi, *Estimation of the price elasticity of petroleum products' consumption in Ukraine*, in *Equilibrium Quarterly Journal of Economics and Economic Policy*, 2020, Vol. 15, No. 2, pp. 315–339; J. Hasanova, K. Najafova, *Development of trade-economic relations between Azerbaijan–EU countries in the field of natural gas supply*, in *WSEAS Transactions on Business and Economics*, 2024, Vol. 21, pp. 1104–1114; A. Huseynova, O. Mazanova, P. Khudiyeva, H. Muradova, H. Leyla, N. Kamala, *Innovative way of solution of "Smart City" in Azerbaijan – city problems*, in *WSEAS Transactions on Business and Economics*, 2022, Vol. 19, pp. 1394–1402.

129 A. Mohammed, *Cybersecurity in smart cities: As cities become smarter, new vulnerabilities arise. Research can focus on securing IoT devices, smart infrastructure, and privacy concerns associated with smart city*

how the protection of urban infrastructure and citizens' data becomes central to ensuring a safe and sustainable urban environment (SDG 11).

Thus, the study demonstrated that the national cybersecurity models developed constitute an adequate response to existing threats as identified by both governmental and academic stakeholders. At the same time, a gap has been revealed between high-level legislative requirements and the complexity of their technical implementation, which underscores the critical importance of advancing innovative technologies (AI, blockchain, Endpoint Detection and Response (EDR), Extended Detection and Response (XDR)) and deepening cooperation between the state and the technology sector. The success of national strategies will depend on their ability to flexibly adapt to emerging threats, such as hardware-level attacks, and how effectively they can integrate cybersecurity into the broader context of achieving national and global SDGs.

5. Conclusions

The research established that despite the presence of shared challenges arising from the globalisation of cyber threats (the escalation of which was reported by 72% of organisations), each country develops its own unique governance model that reflects its legal, political, and security context. The analysis identified three such models: the European harmonised model (Poland and the Netherlands), which evolves in line with EU directives such as NIS2 and is aimed at standardising requirements and creating a predictable single digital market; the Ukrainian resilience model under wartime conditions, where military cyber defence and the mobilisation of all available resources to counter direct aggression are prioritised, as reflected in the creation of military cyber forces and the investigation of cyberattacks as war crimes; and the Canadian federal model based on partnership, where responsibility is distributed between the federal and provincial levels (which account for 51% of public investment), and protection is ensured through a combination of legislation and voluntary certification programmes for businesses. The study confirmed that, regardless of the chosen model, all states recognise the strategic importance of protecting critical infrastructure, the necessity of close public-private cooperation, and the strengthening of international collabora-

data, in *Pioneer Research Journal of Computing Science*, 2024, Vol. 1, No. 1, pp. 75-82.

tion to effectively counter threats.

The practical significance of the results lies in the formulation of a set of recommendations for improving national policies. For countries in the process of developing their cybersecurity systems, it is advisable to apply a hybrid approach that synthesises best practices from various models: adopting clear regulatory standards for operators from the European model; implementing crisis protocols and mobilisation mechanisms tested in Ukraine; and introducing a multi-level coordination system modelled after Canada's experience to involve regional authorities and businesses. For established systems, it is recommended to strengthen dialogue with representatives of the technology industry and critical infrastructure operators already at the stage of regulatory drafting, in order to avoid the creation of regulatory frameworks that are technically difficult to implement and to reduce the gap between legislative intent and practical implementation. For international organisations and alliances such as the EU, it is recommended to establish platforms for the exchange of experience not only on the technical aspects of cyber threats but also on the effectiveness of various models of public administration. Promising avenues for further scientific inquiry include conducting quantitative research aimed at assessing the correlation between specific models of state regulation and the actual level of security, including an analysis of the economic impact of incidents across different jurisdictions.