UDC 351.746.1:004.056(477):341.24 **doi:** https://doi.org/10.20998/3083-6298.2025.03.05

Olena Krainiuk[1], Serhii Yevseiev[2], Natali Didenko[1], Mykhailo Piksasov[1]

[1] Kharkiv national automobile and highway university, Kharkiv, Ukraine
[2] National Technical University "Kharkiv polytechnic institute", Kharkiv, Ukraine

TRANSFORMATION OF THE REGULATORY AND LEGAL FRAMEWORK FOR CYBERSECURITY IN UKRAINE: ANALYSIS OF COMPLIANCE WITH THE REQUIREMENTS OF THE NIS2 DIRECTIVE AND THE CYBERSECURITY ACT

Abstract. Topicality. Ukraine's national security is critically dependent on its cyber resilience due to Russia's hybrid aggression targeting critical infrastructure. The country's status as an EU candidate requires urgent harmonisation of its cybersecurity policy with the acquis (NIS2 Directive, Cybersecurity Act) while integrating lessons from real-time cyber warfare. **The subject of study** is the evolution of Ukraine's state cybersecurity policy, its institutional architecture, and the regulatory alignment with the EU framework. **The purpose of this article** is to analyse the complex policy transformation – from reactive aggression response to proactive Euro-integration – and to develop a comprehensive Roadmap for regulatory and organisational improvement to enhance national cyber resilience. **Results.** Russian aggression is confirmed as the leading catalyst for legislative evolution (Law of 2017) and the institutional shift towards resilience (post-2022). A comparative analysis revealed low harmonisation in cybersecurity certification (Cybersecurity Act) and collective defence (Cyber Solidarity Act). Systemic problems identified include personnel deficit, institutional friction (DSSSZI/SBU), and the absence of a unified TIS platform. The proposed Roadmap prioritises NIS2 implementation, certification reform, and institutionalising cyber solidarity. **Conclusion.** Despite its robust foundations, Ukraine's cybersecurity system faces significant challenges due to resource deficits and coordination gaps. Successful Euro-integration and counteraction to threats require complex reforms, focusing on regulatory alignment and enhancing collective cyber resilience as detailed in the Roadmap.

Keywords: national cybersecurity, NIS2 directive, EU acquis, critical infrastructure, cyber resilience, CERT-UA, harmonisation of legislation, institutional architecture.

Introduction

Problem relevance. Contemporary global security is defined by the rapid growth of cyberspace as an inseparable arena for geopolitical confrontation. For Ukraine, which has been under constant military and information-technical aggression from the Russian Federation since 2014, cybersecurity has acquired the status of a critical element of national resilience. The topicality of this research is twofold: firstly, Ukraine possesses a unique global experience in countering state-sponsored cyberattacks amid full-scale war, which provides essential empirical material for developing effective protection models at a worldwide level. Secondly, Ukraine's status as a candidate country for EU membership requires the urgent harmonisation of national legislation and institutional architecture with the acquis communautaire of the European Union, particularly the NIS2 Directive and the Cybersecurity Act.

The subject of this study is the current state of Ukraine's cybersecurity policy, its institutional architecture, evolution during military conflict, and the level of regulatory alignment with EU standards. Despite a robust legislative foundation, the practical implementation of this policy is hampered by several systemic unresolved issues that require in-depth scientific analysis. These include the need to clarify powers and enhance inter-agency coordination, personnel deficits in the state sector, and the lack of a unified, internationally recognised cybersecurity certification mechanism, which impedes the integration of Ukrainian IT products into the European market.

The purpose of the article is to analyse the complex transformation of Ukraine's cybersecurity policy – from reactive measures against aggression to proactive Euro-integration – and to develop a comprehensive Roadmap of proposals for organisational and regulatory improvement to enhance national cyber resilience.

The purpose of the research. The study aims to conduct a comprehensive analysis of Ukraine's current state cybersecurity policy, assess its transformation under the influence of Russian aggression, and develop an integrated model (roadmap) for improving the national system in line with EU integration requirements and modern cyber threats.

To achieve this aim, the following objectives have been defined:

to analyse the current legal and regulatory framework of Ukraine in the field of cybersecurity and identify the functional powers of the key actors of the national system;

to reveal the transformational impact of Russian aggression (after 2014 and 2022) on the formation of cyber resilience policy and mechanisms of operational response;

to assess the level of harmonisation of Ukrainian legislation with EU law and practice, with particular attention to the NIS2 Directive and the Cyber Solidarity Act;

to identify key problems and obstacles in the practical implementation of cybersecurity policy under wartime conditions;

to develop specific proposals for improving regulatory frameworks, organisational structures, and mechanisms of international cooperation.

1. Literature review

1.1. Overview of the Contemporary Regulatory and Legal Framework of Cybersecurity in Ukraine

The system of regulatory and legal frameworks for cybersecurity in Ukraine is multi-level, constantly evolving under the influence of hybrid aggression and digitalisation.

The key element is the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017), which defined the legal and organisational basis for protecting vital interests in cyberspace and institutionalised the concept of Critical Infrastructure (CI) [1]. The regulatory field is supplemented by specialised laws concerning various aspects of information protection [2], and legal responsibility for cybercrimes is enshrined in Chapter XVI of the Criminal Code of Ukraine. Strategic planning is carried out through Ukraine's Cybersecurity Strategy, which focuses on countering Russian aggression and integrating into EU and NATO structures. Ukraine has ratified the Council of Europe Convention on Cybercrime and actively harmonises legislation with European standards (NIS2, Cybersecurity Act, GDPR) [3]. Still, the integration of international standards into national law remains incomplete [4].

By-laws ensure the detailing of norms. CMU Resolutions regulate CI protection and define requirements for State Information Systems, while the Normative documents of the State Service of Special Communications and Information Protection (DSSSZI) establish technical requirements for developing Comprehensive Information Protection Systems (CIPS/KSZI). Among the key problems are fragmentation, inconsistency in terminology and mandates between agencies, insufficient adaptation to new technologies (such as AI and blockchain), and weak integration of international standards. The need to increase the cyber literacy of the population is a pressing issue [5]. Recommendations for improvement include harmonisation of legislation with NIS2, human capital development, and expansion of international cooperation [6, 7].

1.2. Institutional architecture and distribution of functional powers in the national cybersecurity system

The effectiveness of national cybersecurity is ensured by a multi-level institutional system, where the key architectural principles are coordination, avoidance of overlapping mandates, and interagency cooperation [8, 9]. Strategic management of the system is carried out by the National Security and Defence Council of Ukraine (NSDC), which defines the fundamental policy directions and coordinates all actors (Table 1).

Table 1 – **National Cybersecurity System of Ukraine**

Entity	Key Authorities
National Security and Defense Council of Ukraine (NSDC)	Defines key directions and strategy, and coordinates the activities of system actors. Makes decisions on the imposition of sanctions.
State Service of Special Communications and Information Protection of Ukraine (SSSCIP)	The key authority responsible for developing and implementing state cybersecurity policy. Exercises state control over the cybersecurity posture, ensures the functioning of the National Center for Operational and Technical Management of Telecommunications Networks (NCOC) and the Government Computer Emergency Response Team of Ukraine (CERT-UA). Responsible for protecting state information resources and communication systems.
Security Service of Ukraine (SSU)	Counterintelligence protection of state interests in cyberspace. Detection, prevention, and suppression of cybercrimes that threaten national security. Conducts cyber intelligence.
Ministry of Defense of Ukraine / General Staff of the Armed Forces of Ukraine	Ensures cybersecurity of military information systems, cyber defense, and conducts cyber operations in the military domain.
National Bank of Ukraine (NBU)	Ensures cybersecurity of Ukraine’s banking and financial system. Establishes requirements for financial institutions.
National Police of Ukraine (NPU)	Investigates cybercrimes that do not threaten national security (fraud, unauthorized access).
Ministry of Digital Transformation of Ukraine	Develops policies in the field of digital transformation, expands electronic services and registries, and initiates regulatory frameworks.

The central elements of the system are distributed according to their functional missions:

the State Service of Special Communications and Information Protection (SSSCIP) is the central authority responsible for developing and implementing cybersecurity policies, overseeing operational structures, including CERT-UA (the incident response unit);

the Security Service of Ukraine (SSU) performs the function of counterintelligence protection of national interests in cyberspace, focusing on detecting and preventing cybercrimes that threaten national security, as well as conducting cyberintelligence;

specialised structures ensure the protection of individual sectors: the Ministry of Defence/General Staff of the Armed Forces of Ukraine carry out cyber defence; the National Bank of Ukraine regulates cybersecurity of the financial system; the National Police investigates general criminal cyber offences; and the Ministry of Digital Transformation acts as a policy driver of digitalisation.

Thus, the national system operates as a distributed and hierarchically subordinated structure, where strategic decisions of the NSDC are implemented through specialised operational and sectoral bodies.

The Ministry of Digital Transformation develops digital transformation policy, expands electronic services and registries, and initiates regulatory measures.

To illustrate the functional distribution and multi-level structure of national cybersecurity, a Conceptual Model of the institutional architecture was developed. As shown in Fig. 1, the system is hierarchical: the strategic level is represented by the NSDC (NCCC); the middle level includes the SSSCIP, SSU, MoD and the NBU; and the lower level consists of critical infrastructure assets. The model demonstrates subordination, coordination, and potential overlaps in mandates, particularly between the SSSCIP and the SSU.

Despite the defined structure, policy implementation faces systemic challenges. A key issue is insufficient detail and partial inconsistency in the mandates of operational actors, which at times leads to overlapping functions or "grey zones" of responsibility during responses to hybrid incidents [10]. Another pressing need is the accelerated adaptation of national protocols and standards to meet NATO and EU requirements, ensuring interoperability [3]. These gaps are exacerbated by a shortage of highly qualified personnel in the public sector, which limits the deployment of innovative solutions and the ability to counter dynamic cyber threats [11]. Additional problems include a fragmented regulatory framework, weak private-sector integration, low public cyber literacy, and limited interagency information sharing [12].

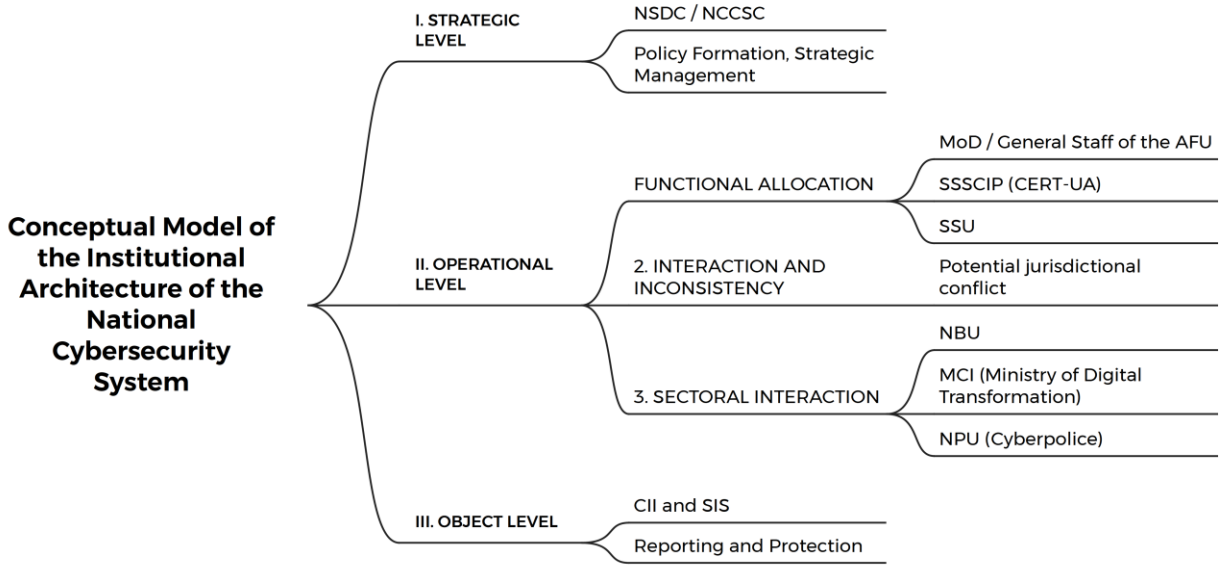

Fig. 1. Conceptual model of the institutional architecture of the National Cybersecurity System of Ukraine

The institutional architecture is complex, but it requires further clarification of mandates, strengthened coordination, and harmonisation with NATO/EU standards. Improving effectiveness is possible through refining the roles of actors, developing human capital, and enhancing interagency cooperation.

2. Influence of Russian Aggression on the Transformation of National Cybersecurity Policy

Russian aggression has become the key catalyst for changes in Ukraine's national cybersecurity policy, which has evolved in two phases corresponding to the escalation of the war.

After 2014, Ukraine faced large-scale, state-sponsored cyber operations integrated into hybrid warfare, which necessitated the institutionalisation of its cybersecurity system [13, 14]. Data (Fig. 2) confirm that aggression is the primary driver of transformation: in 2022, the number of attacks increased by 62.5%, and in 2024, by nearly 70%. In response, the state adopted the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017). It strengthened CERT-UA and the National Telecommunications Network Operations Centre (NTCU), enabling centralised monitoring and response. A turning point was the Petya/NotPetya incident (2017) [15, 16], which exposed critical vulnerabilities in the private sector and demonstrated the need to protect essential infrastructure regardless of ownership.

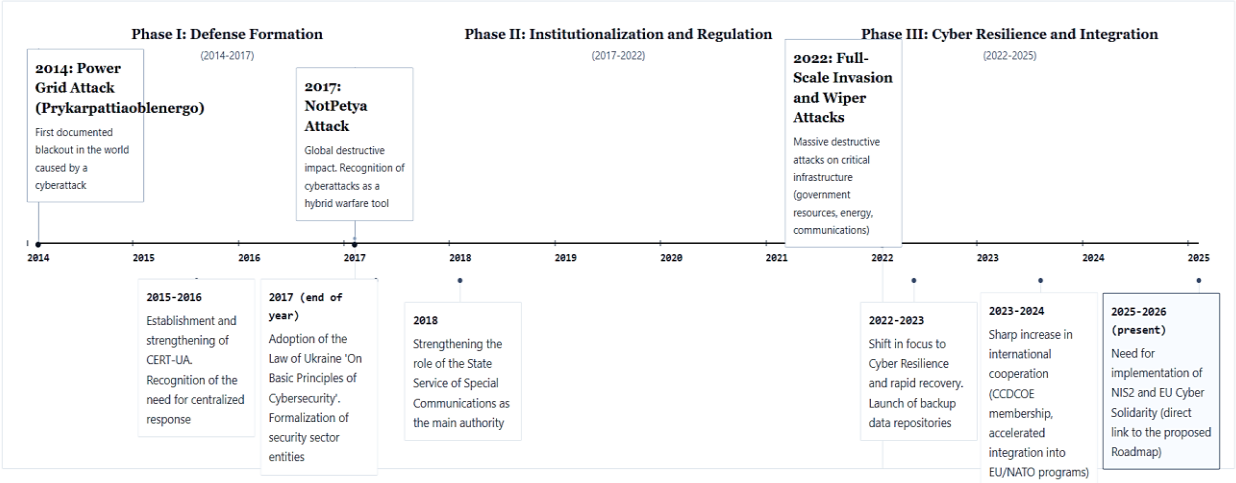

Fig. 2. Analysis of correlation cycles (resource, institutional, regulatory) affecting the level of cyber resilience of the national system

The full-scale invasion triggered a shift to a "military" cybersecurity model (Fig. 3, 4), focusing primarily on resilience and continuity rather than prevention alone. The powers of the State Service of Special Communications (SSSCIP) over critical infrastructure were expanded, and the Ministry of Defence intensified the development of cyber forces.

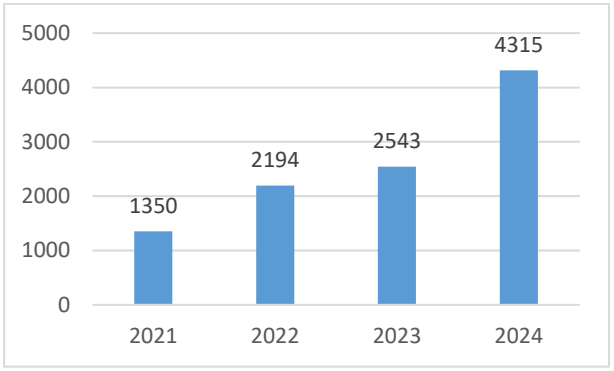

Fig. 3. Dynamics of the total number of incidents (Total Registered Cyber Incidents) (based on data from [20])

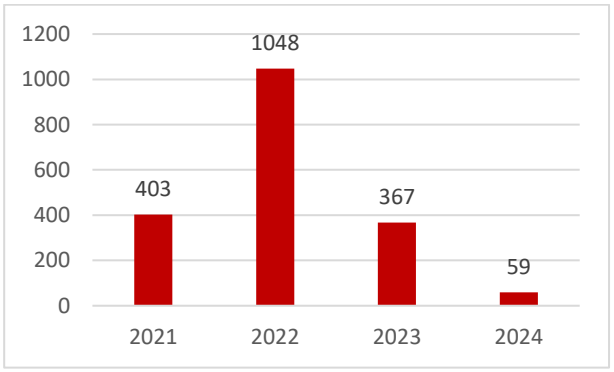

Fig. 4. Dynamics of Critical and High-level Cyber Incidents

International cooperation deepened significantly, with Ukraine receiving technical, operational, and expert support from the US, EU, and NATO. Study [17] highlights the role of CERT-UA, cooperation with the United States, and the importance of legal reforms.

A distinctive feature of this period was the emergence of informal mechanisms such as the "IT Army" [18, 19], which, although outside official state policy, has a notable impact on cyber defence and the information space.

The dynamics of critical incidents handled by CERT-UA reveal a clear shift in the aggressor's strategy and an increasing cyber resilience in Ukraine. The 2022 peak (1048 incidents) reflects a phase of destructive wipe-out attacks targeting critical infrastructure. The sharp decline in 2023 and 2024 (to 367 and 59 incidents) does not indicate a reduction in threats, but rather a tactical shift toward espionage-focused CNE operations, highlighting the effectiveness of Ukraine's strengthened resilience and international cooperation. This confirms the need for continuous adaptation of national cybersecurity policy.

Russian aggression has become a catalyst for the evolution of Ukraine's cyber policy, making it one of the most experienced and adaptive worldwide in countering state-sponsored cyberattacks. The accumulated experience forms a solid empirical basis for further harmonisation with Western standards and the development of an integrated cyber resilience system.

3. Assessment of the level of harmonization of national legislation with European Union law and practice

Ukraine's EU integration path requires substantial alignment of cybersecurity norms with the EU acquis, primarily NIS2, the Cybersecurity Act, and initiatives such as the Cyber Solidarity Act. To identify gaps, a comparative matrix was developed (Table 1), visualising the level of compliance and critical areas for reform. A summary assessment is provided in Table 2.

NIS2 establishes unified cybersecurity standards for critical sectors in the EU. Analysis shows partial compliance in Ukraine, but several areas require further development:

1. Classification of entities. Ukraine's list of critical infrastructure assets (CIAs) is less detailed than the NIS2

categorisation into essential and vital, requiring broader coverage of critical sectors [4].

2. Risk management and reporting. Although requirements for Information Security Management Systems (ISMS) exist, incident reporting mechanisms do not fully meet NIS2's strict timelines and standards, indicating a medium level of harmonisation [21].

3. International cooperation. Ukraine actively engages internationally but lacks full integration with the European CERT/CSIRT network, resulting in a low to medium level of compliance [22].

The Cybersecurity Act aims to create a unified EU system for certifying the cybersecurity of products, services, and processes. Ukraine's current certification system, under the jurisdiction of SSSCIP, does not ensure automatic recognition in the EU, creating a technical barrier for IT products. Complete reform of the national certification system is needed to comply with the Regulation [4, 23].

The Cyber Solidarity Act strengthens joint threat detection (European Cyber Shield) and rapid response mechanisms. Ukraine receives international support but is not a full participant, resulting in low harmonisation. Full integration requires legal and infrastructural alignment with European structures and real-time data-sharing platforms [24, 25].

Ukraine's legislation provides a solid institutional and regulatory foundation, but achieving EU integration goals requires substantial refinement to fully comply with NIS2 and implement a certification system recognised by the EU under the Cybersecurity Act [24].

Table 2 – **Assessment of the Alignment of Ukraine's State Cybersecurity Policy with EU Standards**

EU Legal Act	Key Requirement / Area	Status in Ukraine (Current State)	Harmonisation Level	Priority for the Roadmap
NIS2 Directive	1. Classification of CIAs (Essential / Important)	A list of critical infrastructure assets exists, but it is less detailed and does not cover all categories of "important" entities.	Medium	High (Expansion of regulatory scope required)
NIS2 Directive	2. Risk management and reporting (Unified deadlines)	Requirements for ISMS exist (CMU Resolutions), but reporting mechanisms are less standardised and do not meet NIS2 strict timelines.	Medium	High (Standardisation of requirements and deadlines)
NIS2 Directive	3. International cooperation (CSIRT Network)	Bilateral cooperation exists, but no integrated national mechanism for interaction with the EU CSIRT network.	Low/Medium	High (Legislative consolidation of mechanisms)
Cybersecurity Act	Certification of cyber products (Recognition in the EU)	Ukraine's certification system (SSSCIP) exists but does not ensure automatic recognition in the EU.	Low	Critical (Complete system reform required)
Cyber Solidarity Act	Cyber solidarity mechanisms (Reserves, rapid response)	Ukraine receives assistance but is not a full participant and lacks an institutionalised national resource reserve.	Low	Critical (Infrastructure and legal integration)

4. Key Challenges in the Practical Implementation of Cybersecurity Policy

Despite an established legal framework, the implementation of cybersecurity policy in Ukraine is hindered by systemic issues exacerbated by the war.

1. Workforce Shortage. The public sector faces an acute shortage of specialists and loses market share to private companies, resulting in an outflow of expertise and hindering modernisation [26].

2. Insufficient Financial and Technological Resources. Limited funding prevents the renewal of equipment and software, making regional systems vulnerable and hindering compliance with NIS2 requirements [27, 28].

3. Overlapping Mandates and Weak Coordination. The unclear division of responsibilities between the SBU and SSSCIP hinders incident response. Establishing a unified coordination centre is necessary [10].

4. Low Cyber Hygiene of Non-state Critical Infrastructure Operators. Private operators often comply only formally, creating risks of cascading failures across critical infrastructure. Audits and improvements in cybersecurity culture are needed [29].

5. Lack of a Unified TIS Platform. Automated threat information sharing is absent; interaction is fragmented and not integrated with international systems. This delays IoC detection and reduces the effectiveness of collective defence.

6. Other Systemic Issues:

low digital maturity of public institutions. Outdated architectures and a formal approach to ISMS impede the adoption of security by design;

gaps in cloud service regulation. Uncertainty regarding security, outsourcing, and data control poses risks to the sovereignty of state information, particularly when utilising foreign cloud services [30];

weak counteraction to information and psychological operations. Responses to hybrid attacks are fragmented, and coordination between technical and information structures is insufficient [31];

insufficient readiness for post-attack recovery. Ukraine lacks national cyber reserves and mechanisms for the the rapid restoration of critical infrastructure systems, contrary to the approaches outlined in the Cyber Solidarity Act [32].

These interconnected issues form negative cycles that hinder the enhancement of national cyber resilience.

As illustrated in Fig. 5, the challenges related to financial and workforce shortages are not independent of institutional misalignment and regulatory gaps. They reinforce one another, creating three key correlation cycles: the resource deficit cycle, the institutional dysfunction cycle, and the regulatory adaptation cycle. The interaction of these cycles results in a persistently low level of cyber resilience (central node), demonstrating the need for a comprehensive rather than a fragmented approach to policy improvement.

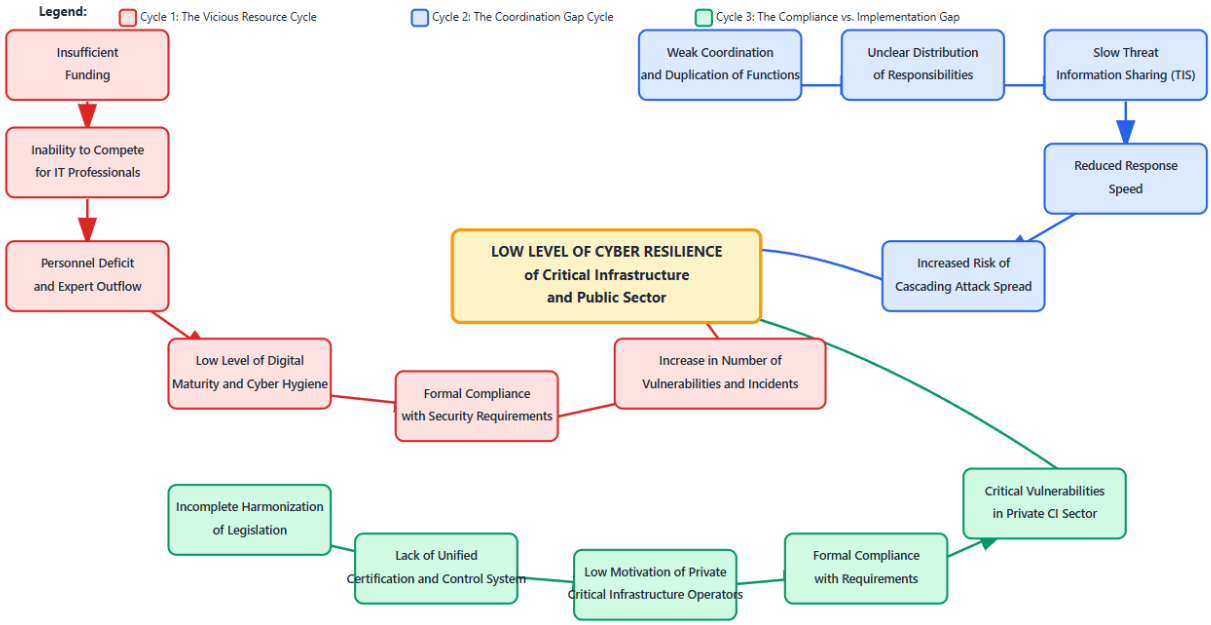

Fig. 5. Analysis of correlation cycles affecting the level of cyber resilience of the national system

5. Roadmap for Improving Ukraine's Cybersecurity Policy

Enhancing the national cybersecurity system requires alignment with EU law and strengthening the resilience of critical infrastructure.

Stage 1. Regulatory Framework (EU Harmonisation).

1.1. NIS2 Implementation. Full adaptation of the Law of Ukraine on the Basic Principles of Cybersecurity to NIS2 requirements: Essential/Important classification, unified risk-management and reporting standards.

1.2. Certification Reform (Cybersecurity Act). Transition to independent audits and EU-compatible certification schemes (EUCC, Common Criteria).

1.3. Legal Framework for Cyber Defence. Defining the powers of civilian and military structures and regulating active measures in cyberspace.

Stage 2. Organisational Structure and Workforce.

2.1. Development of CERT-UA. Transformation into a national TIS hub with automated IoC-exchange platforms for cooperation with the private sector and EU CSIRTs.

2.2. Workforce Incentives. Competitive compensation mechanisms, national internship and scholarship programs to form a skilled talent pool.

2.3. Independent CI Audits. Legal requirements for periodic cybersecurity audits of critical infrastructure conducted by licensed private companies under the supervision of the State Service for Special Communications.

Stage 3. Response Mechanisms and Resilience.

The focus of this stage is strengthening operational resilience, enabling rapid recovery after attacks, and integrating with European cyber-solidarity mechanisms.

3.1. National Cyber Resilience Program. Creation of a state backup system for critical registries with geographically distributed storage, including international locations. The goal is to ensure continuity of government services in the event of cyberattacks or physical destruction.

3.2. EU Cyber Solidarity Instruments. Establishment of national equipment reserves and rapid-response expert teams aligned with the Cyber Solidarity Act to restore critical infrastructure after large-scale attacks.

3.3. National Cyber Exercises. Implementation of annual exercises simulating crisis scenarios (wiper attacks, telecom blackouts) with the participation of critical infrastructure operators, the private sector, government bodies, and international partners.

Table 3 – **Roadmap for Improving Ukraine's Cybersecurity Policy (2025–2027)**

Stage	Direction	Measure	Key Goal (Outcome)	Responsible Entities
Stage 1: Regulatory Framework (Harmonization)	EU Legal Alignment	1.1. Implementation of NIS2	Adoption of amendments to the Cybersecurity Law; unification of CI classification (Essential/Important) and requirements for risk management and reporting.	SSSCIP, Ministry of Digital Transformation, NSDC
	Regulatory Policy	1.2. Certification Reform (Cybersecurity Act)	Introduction of an EU-recognized certification system; transition to independent audits and voluntary product certification.	SSSCIP, Ministry of Economy
	Cyber Defence	1.3. Establishing a Legal Regime for Cyber Defence	Clear definition of MoD/General Staff authority regarding active cyber operations (offensive/active measures).	MoD, NSDC, Security Service of Ukraine
Stage 2: Organizational Structure and Workforce	Operational Efficiency	2.1. Strengthening CERT-UA	Transformation of CERT-UA into a national TIS hub (cyber threat intelligence exchange) with automated integration into European CSIRTs.	SSSCIP
	Human Resources	2.2. Introduction of a Financial Incentive System	Development of a competitive mechanism of bonuses/allowances for highly qualified specialists in the public sector.	Cabinet of Ministers, Ministry of Finance
	Quality Control	2.3. Continuous CI Audits	Legal establishment of mandatory independent cybersecurity audits of critical infrastructure by licensed private companies.	SSSCIP, Ministry of Digital Transformation
Stage 3: Response Mechanisms and Resilience	Business Continuity	3.1. National Cyber Resilience Program	Creation of national backup repositories (backup cloud) for critical registries, including geographically distributed storage.	Cabinet of Ministers, Ministry of Digital Transformation
	Resource Capacity	3.2. Implementation of EU Cyber Solidarity Instruments	Establishment of national reserves of equipment and experts for rapid CI recovery in case of large-scale attacks.	SSSCIP, Cabinet of Ministers
	Operational Readiness	3.3. Regular National Cyber Exercises	Annual nationwide exercises involving CI operators, private sector and international partners (wiper and blackout scenario training).	NSDC, SSSCIP

Discussion of results

The findings highlight that Ukraine's cybersecurity policy continues to evolve under the dual pressure of ongoing hybrid threats and the strategic imperative of EU integration. The shift from reactive defence against large-scale destructive cyberattacks to a resilience-oriented model reflects both the maturation of national institutions and the changing tactics of hostile actors. At the same time, the analysis demonstrates that regulatory misalignment with key EU instruments — particularly in certification and collective cyber defence — remains a major barrier to integration. Persistent structural challenges, such as institutional overlaps and limited cybersecurity workforce capacity, further hinder effective policy implementation. These results underscore the need for a coordinated and multi-level reform effort, where legislative harmonisation, organisational restructuring, and the development of national threat-intelligence capabilities are treated as interconnected components of a unified cybersecurity modernisation strategy.

Conclusions

Based on the analysis of Ukraine's national cybersecurity policy, its transformation under Russian aggression, and the assessment of harmonisation with EU law, the following key conclusions were drawn:

1. Russian aggression is the primary catalyst for the evolution of national cybersecurity policy, leading to a qualitative shift towards a cyber resilience regime and a change in the aggressor's tactics from destructive attacks (CNA) to espionage operations (CNE).

2. A low level of harmonisation of Ukrainian legislation with the EU acquis has been identified in critical regulatory areas, particularly regarding cybersecurity product certification (Cybersecurity Act) and participation in Cyber Solidarity mechanisms (Cyber Solidarity Act).

3. Practical implementation of policy is constrained by systemic issues, including workforce shortages, institutional fragmentation (conflicts between SSSCIP and SBU), and the absence of a unified national Threat Intelligence Sharing (TIS) platform.

To overcome these systemic deficits and achieve EU integration goals, it is necessary to implement a comprehensive Roadmap, prioritising full NIS2 implementation, certification system reform, and institutionalisation of cyber solidarity mechanisms.

References

1. Bodunova, O. and Topchii, V. (2025), "Problematic issues of ensuring cybersecurity in Ukraine", *Analytical and Comparative Jurisprudence.* URL: https://doi.org/10.24144/2788-6018.2025.01.110
2. Sopilko, I. and Cherevatiuk, V. (2022), "Cyber security and personal rights under the legislation of Ukraine", *Journal of International Legal Communication*. pp. 18–25, doi: https://doi.org/10.32612/uw.27201643.2022.6.pp.18-25
3. Shopina, I., Khomiakov, D., Khrystynchenko, N., Zhukov, S. and Shpenov, D. (2020), "Cybersecurity: legal and organizational support in leading countries, NATO and eu standards", *Journal of Security and Sustainability Issues*, vol. 9, pp. 977–992, doi: https://doi.org/10.9770/jssi.2020.9.3(22)
4. Zubok, V., Davydiuk, A. and Klymenko, T. (2023), "Cybersecurity of Critical Infrastructure in Ukrainian Legislation and in Directive (EU) 2022/2555", *Èlektronnoe modelirovanie*, vol. 45, pp. 54–63, doi: https://doi.org/10.15407/emodel.45.05.054
5. Horulko, V. (2025), "Main directions of improving Ukrainian legislation on information security in war conditions", *Uzhhorod National University Herald*. Series: Law, doi: https://doi.org/10.24144/2307-3322.2025.88.2.49
6. Kovaliv, M., Skrynkovskyy, R., Nazar, Y., Yesimov, S., Krasnytskyi, I., Kaydrovych, K., Kniaz, S. and Kemska, Y. (2021), "Legal Support of Cybersecurity of Critical Information Infrastructure of Ukraine", *Path of Science*, vol. 7, pp. 2011–2018, doi: https://doi.org/10.22178/pos.69-12
7. Lyseiuk, A. and Svintsitska, T. (2024), "Development of International Cooperation in Cybersecurity: Normative and Legal Framework and Prospects", *Law and innovative society*, doi: https://doi.org/10.37772/2309-9275-2024-2(23)-8
8. Svintsytskyi, A. (2022), "The system of cybersecurity bodies in Ukraine", *Revista Científica General José María Córdova*, doi: https://doi.org/10.21830/19006586.903
9. Vasylenko, V. (2025), "National Cybersecurity in the Context of Society Digitalization: the Role of Police in Protecting Critical Infrastructure", *Bulletin of Kharkiv National University of Internal Affairs*, doi: https://doi.org/10.32631/v.2025.2.33
10. Tarasenko, O., Mirkovets, D., Shevchyshen, A., Nahorniuk-Danyliuk, O. and Yermakov, Y. (2022), "Cyber security as the basis for the national security of Ukraine", *Cuestiones Políticas*, doi: https://doi.org/10.46398/cuestpol.4073.33
11. Fischer-H¨ubner, S., Alcaraz, C., Ferreira, A., Fernández-Gago, C., López, J., Markatos, E., Islami, L. and Akil, M. (2021), "Stakeholder perspectives and requirements on cybersecurity in Europe", *J. Inf. Secur. Appl*., vol. 61, p. 102916, doi: https://doi.org/10.1016/j.jisa.2021.102916
12. Savchuk, S. (2024), "Challenges and prospects for the formation of state policy in the field of cybersecurity and combating cybercrime", *Public Policy and Accounting*, doi: https://doi.org/10.26642/ppa-2024-1(9)-30-38
13. Takamaa, M. and Lehto, M. (2024), "Cyber Operations in Ukraine: Emerging Patterns in Cases", European Conference on Cyber *Warfare and Security*, doi: https://doi.org/10.34190/eccws.23.1.2122
14. Duda, D. and Kowalska, J. (2024), "The concept of warfare in cyberspace as an example of hybrid warfare of the russian federation", *National Security Studies*, doi: https://doi.org/10.37055/sbn/196886
15. Orlovskyi, R. and Kozak, V. (2025), "Criminal law protection of state secrets in the context of hybrid warfare", *Kriminologija & socijalna integracija*, doi: https://doi.org/10.31299/ksi.33.1.5
16. Priyono, U. (2022), "Cyber warfare as part of russia and Ukraine conflict", *Jurnal Diplomasi Pertahanan*, doi: https://doi.org/10.33172/jdp.v8i2.1005
17. Sarimin, B. and Damayanti, A. (2024), "Ukraine's Strategy to Counter Russian Cyber Threats in the Russo–Ukrainian War", *International Journal of Social Science and Human Research*, doi: https://doi.org/10.47191/ijsshr/v7-i11-37
18. Zulfian, M. and Rahmadan, Y. (2025), "Analyzing Russia's Hybrid Warfare Strategy through HermeticWiper Against Ukraine: A Cybersecurity and Desecuritization Approach", *Journal of Public Administration and Political Science and International Relations*, doi: https://doi.org/10.61978/politeia.v3i3.673
19. Fedotenko, K. (2023), "Cyber warfare as part of information warfare of russia against Ukraine since the beginning of the 2022 russian invasion", *Věda a perspektivy*, pp. 351–357, doi: https://doi.org/10.52058/2695-1592-2023-8(27)-351-357
20. State Service of Special Communications and Information Protection of Ukraine, International Cyber Environment Task Force. (2025), "War and Cyber: Three Years of Struggle and Lessons for Global Security", *Analytical report*, Kyiv, pp. 21, URL: https://cip.gov.ua/services/cm/api/attachment/download?id=69131
21. Chiara, P. (2024), "Towards a right to cybersecurity in EU law? The challenges ahead", *Comput. Law Secur. Rev*., vol. 53, p. 105961, doi: https://doi.org/10.1016/j.clsr.2024.105961
22. Nazarenko, S., Sharyi, V. and Kifin, O. (2024), "Prospects for the integration of Ukraine's national security mechanisms with the collective security systems of the EU and NATO", *Economic scope*, pp. 55–59, doi: https://doi.org/10.30838/ep.194.55-59
23. Khurshid, A., Alsaaidi, R., Aslam, M. and Raza, S. (2022), "EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme", *IEEE Access*, vol. 10, pp. 129932–129948, doi: https://doi.org/10.1109/access.2022.3225973
24. Villani, S. (2025), "The Cyber Solidarity Act: Framework and Perspectives for the New EU-Wide Cybersecurity Solidarity Mechanism Under the EU Legal System", *European Journal of Risk Regulation*, doi: https://doi.org/10.1017/err.2025.24
25. Dewi, A. and Nugrahani, H. (2024), "Strengthening EU Cyber Resilience: A Critical Analysis of the Cyber Solidarity Act's Legislative Framework", *Journal of World and Politics*, doi: https://doi.org/10.18196/jiwp.v8i2.115
26. Prokopovych-Tkachenko, D., Zvieriev, V. and Kozachenko, I. (2025), "Integration of Security Operations Centers (SOC) into Ukraine's national security system", *STATE SECURITY*, doi: https://doi.org/10.33405/2786-8613/2025/1/5/336736

27. Semenenko, O., Kin, O., Zaitsev, O., Tkach, I. and Kuravskyi, V. (2025), "The impact of digital technologies on the defence economy of Ukraine in the context of economic challenges to cybersecurity", *Economics of Development*, doi: https://doi.org/10.63341/econ/1.2025.118
28. Guitton, M. and Frechette, J. (2023), "Facing cyberthreats in a crisis and post-crisis era: Rethinking security services response strategy", *Computers in Human Behavior Reports*, vol. 10, p. 100282, doi: https://doi.org/10.1016/j.chbr.2023.100282
29. Davydiuk, A. and Zubok, V. (2023), "Analytical Review of the Resilience of Ukraine's Critical Energy Infrastructure to Cyber Threats in Times of War", 2023 *15th International Conference on Cyber Conflict*: *Meeting Reality* (CyCon), pp. 121–139, doi: https://doi.org/10.23919/cycon58705.2023.10181813
30. Nugraha, Y. and Martin, A. (2022), "Cybersecurity service level agreements: understanding government data confidentiality requirements", *Journal of Cybersecurity*, vol. 8, doi: https://doi.org/10.1093/cybsec/tyac004
31. Khriapynskyi, A. (2024), "Perspective directions of information policy for countering hybrid threats", *State Formation*, doi: https://doi.org/10.26565/1992-2337-2024-2-22
32. Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A. and Hutchison, D. (2022), "A cyber incident response and recovery framework to support operators of ICS and Critical National Infrastructure", *International Journal of Critical Infrastructure Protection*, doi: https://doi.org/10.1016/j.ijcip.2021.100505

Received (Надійшла) 18.11.2025
Accepted for publication (Прийнята до друку) 26.11.2025

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Крайнюк Олена Володимирівна – кандидат технічних наук, доцент, Харківський національний автомобільно-дорожній університет, Харків, Україна;
Olena Krainiuk – PhD, Associate Professor, Kharkiv national automobile and highway university, Kharkiv, Ukraine;
e-mail: olenakrainiuk@khadi.kharkov.ua; ORCID Author ID: https://orcid.org/0000-0001-9524-040X;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=59134516300.

Євсеєв Сергій Петрович – доктор технічних наук, професор, завідувач кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Serhii Yevseiev – Doctor of Technical Sciences, Professor, Head of Cyber Security Department, National Technical University "Kharkiv polytechnic institute", Kharkiv, Ukraine;
e-mail: Serhii.Yevseiev@gmail.com; ORCID Author ID: https://orcid.org/0000-0003-1647-6444;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57190440690.

Діденко Наталя Вікторівна – кандидат технічних наук, доцент, Харківський національний автомобільно-дорожній університет, Харків, Україна;
Natalia Didenko – PhD, Associate Professor, Kharkiv national automobile and highway university, Kharkiv, Ukraine;
e-mail: nataly.v.didenko@gmail.com; ORCID Author ID: https://orcid.org/0000-0003-3318-438X;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57219057398.

Піксасов Михайло Михайлович – кандидат технічних наук, доцент, Харківський національний автомобільно-дорожній університет, Харків, Україна;
Mykhailo Piksasov – PhD, Associate Professor, Kharkiv national automobile and highway university, Kharkiv, Ukraine;
e-mail: mpiks77@gmail.com; ORCID Author ID: https://orcid.org/0000-0001-9487-7273.

ТРАНСФОРМАЦІЯ НОРМАТИВНО-ПРАВОВОГО ПОЛЯ КІБЕРБЕЗПЕКИ УКРАЇНИ: АНАЛІЗ ВІДПОВІДНОСТІ ВИМОГАМ ДИРЕКТИВИ NIS2 ТА ЗАКОНУ ПРО КІБЕРБЕЗПЕКУ

О.В. Крайнюк, С.П. Євсеєв, Н.В. Діденко, М.М. Піксасов

Анотація. Актуальність. Національна безпека України критично залежить від її кіберстійкості через гібридну агресію Росії, спрямовану на критичну інфраструктуру. Статус кандидата в ЄС вимагає невідкладної гармонізації політики кібербезпеки з правовими надбаннями ЄС (директива NIS2, Закон про кібербезпеку) із врахуванням уроків сучасної кібервійни. **Предмет дослідження.** Еволюція державної політики кібербезпеки України, її інституційна архітектура та регуляторна узгодженість із європейською правовою рамкою. **Мета статті.** Проаналізувати складну трансформацію політики – від реактивного реагування на агресію до проактивної євроінтеграції – та розробити комплексну Дорожню карту нормативного та організаційного вдосконалення для підвищення національної кіберстійкості. **Результати.** Російська агресія підтверджена як головний каталізатор еволюції законодавства (Закон 2017 року) та інституційного переходу до кіберстійкості (після 2022 року). Порівняльний аналіз виявив низький рівень гармонізації у сфері сертифікації (Cybersecurity Act) та колективного захисту (Cyber Solidarity Act). Виявлені системні проблеми включають дефіцит кадрів, інституційну фрикцію (ДССЗЗІ/СБУ) та відсутність єдиної платформи TIS. Запропонована Дорожня карта пріоритезує імплементацію NIS2, реформу сертифікації та інституціалізацію механізмів кіберсолідарності. **Висновок.** Незважаючи на міцну законодавчу та інституційну базу, система кібербезпеки України стикається із серйозними викликами через дефіцит ресурсів та прогалини в координації. Успішна євроінтеграція та протидія загрозам потребують комплексних реформ із фокусом на регуляторне узгодження та підвищення колективної кіберстійкості, що деталізовано в Дорожній карті.

Ключові слова: національна кібербезпека, директива NIS2, правові надбання ЄС, критична інфраструктура, кіберстійкість, CERT-UA, гармонізація законодавства, інституційна архітектура.