Systemy Logistyczne Wojsk
Zeszyt 65(2026)
s. 115-132

Instytut Logistyki
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna w Warszawie

Military Logistics Systems
Volume 65(2026)
pp. 115-132

Institute of Logistics
Faculty of Security, Logistics and Management
Military University of Technology in Warsaw

DOI: 10.37055/slw/242082
Article type: Original research article

ISSN 1508-5430
eISSN 2719-7689

CYBERSECURITY AND LEGAL ASPECTS OF CRITICAL INFRASTRUCTURE PROTECTION UNDER GLOBAL THREATS: THE UKRAINIAN PERSPECTIVE

Oleh Semenenko
olehsemenenko4@gmail.com; ORCID: 0000-0001-6477-3414
Institute for Scientific Work, Central Research Institute of the Armed Forces of Ukraine, Ukraine
(Corresponding author)

Ihor Mylashenko
i-mylashenko@hotmail.com; ORCID: 0000-0002-8017-9164
Research Department of Automated Systems, Central Research Institute of the Armed Forces of Ukraine, Ukraine

Maryna Sliusarenko
sliusarenko.m@outlook.com; ORCID: 0000-0003-4165-3908
Research Department for the Development of Operational-Tactical Requirements for Armaments and Military Equipment, Central Research Institute of the Armed Forces of Ukraine, Ukraine

Mykola Linevych
m_linevych@hotmail.com; ORCID: 0009-0005-3904-0581
Research Center for Automated and Unmanned Systems, Central Research Institute of the Armed Forces of Ukraine

Oleksandr Leonenko
oleonenko@outlook.com; ORCID: 0009-0009-1994-438X
Research Center for Automated and Unmanned Systems, Central Research Institute of the Armed Forces of Ukraine

Abstract.
The research gap addressed in this article concerns the limited integration of technical, organisational, and legal dimensions of cybersecurity protection for Ukraine's critical infrastructure in the face of growing global cyber threats and military aggression. The purpose of the research was to assess the current state of cybersecurity in Ukraine's critical infrastructure and to develop an integrated protection model. The study hypothesises that a combination of advanced technological solutions and a robust legal framework can significantly enhance the resilience of critical infrastructure. The methodology involved systematic analysis of national-level cyber risks, the effectiveness of multilayer protection, and international standards in comparison with national regulations. Key findings revealed critical vulnerabilities in Ukraine's energy, transport, financial, and governmental sectors, including inadequate protection of automated control systems, outdated software, limited access control, and a lack of backup communication channels. The findings indicate that multilayer protection, artificial intelligence (AI) systems, and the Zero Trust Model may reduce risks and improve system adaptability. Legal analysis highlighted Ukraine's evolving regulatory framework, which integrates international cybersecurity standards and promotes coordination between the public and private sectors. The article contributes to logistics systems research by linking cyber-resilience with continuity of operations, crisis response, and military readiness. The conclusion emphasises the need for continuous updates to cyber-risk assessment methods and the adoption of advanced technologies like quantum cryptography, AI, and Zero Trust Models to mitigate risks and ensure the resilience of Ukraine's critical infrastructure.

Keywords:
national strategy; artificial intelligence; Zero Trust Model; quantum cryptography; cybersecurity

Introduction

In the current context of rapid digitalisation and globalisation, Ukraine's critical infrastructure – including energy systems, transport, the financial sector, public administration, and other key domains – is becoming increasingly vulnerable to cyberattacks. Large-scale cyber incidents and military aggression underscore the need for not only technical but also legal protection of these systems, including the regulation of liability and international coordination.

A review of the literature on cybersecurity indicates a growing interest among Ukrainian researchers in issues related to the protection of critical infrastructure and the adaptation of the legislative framework to modern cyber threats. Onyshchenko and Hlushko (2022) examine the analytical dimension of Ukraine's cybersecurity in the context of growing external and internal threats. The authors demonstrate that effective cyber risk management requires the integration of state policy, early incident detection systems, and information flow analysis.

The issue of global and local system resilience has become a subject of active research among legal scholars, technologists, and risk management experts. Kumar (2024) emphasises that regulatory acts should be flexible and capable of adapting to rapidly evolving technological risks, highlighting the need to combine legal, organisational, and technical protection measures to enhance system resilience. In turn, Watney (2022) shows that effective protection of critical infrastructure requires a robust legal framework, clear liability and incident-response mechanisms, and

coordinated action among public authorities, the private sector, and international partners. Bechara and Schuch (2021) identify regulatory fragmentation and the lack of unified information-sharing protocols as major obstacles to global critical infrastructure protection, while Malatji et al. (2022) and Lehto (2022) emphasise that cyber-resilience depends on integrating monitoring, threat analysis, incident management, staff training, and coordinated technical, organisational, and legal measures.

Most studies focus separately on technical solutions, legislative regulation, or international practices, lacking a systematic analysis that integrates all these components into a unified model adapted to the specific hybrid threats and national infrastructure features of Ukraine. This study aimed to assess the state of cybersecurity within Ukraine's critical infrastructure and to propose an integrated model for its protection. To achieve this aim, the objectives were to conduct a comprehensive analysis of the current state of Ukraine's critical infrastructure, its cyber components, threat classification, and legal regulation in the field of cybersecurity; and to identify effective technological and organisational solutions for enhancing the cyber-resilience of critical infrastructure and integrating these solutions into the proposed national protection model.

RQ1 examines the key cyber vulnerabilities across Ukraine's critical infrastructure sectors, including energy, transport, finance, public administration, and healthcare. RQ2 investigates the effectiveness of existing national and international regulatory frameworks in ensuring coordinated cybersecurity efforts across public and private sectors. RQ3 explores the impact of advanced technologies like AI-based monitoring, the Zero Trust Model, and quantum cryptography on enhancing the resilience of critical infrastructure. RQ4 assesses how an integrated cybersecurity model, combining technical, organisational, and legal measures, can improve Ukraine's readiness against hybrid cyber threats. The hypothesis of this study is that an integrated cybersecurity model, combining technological solutions, regulatory measures, and organisational coordination, will significantly enhance the resilience of Ukraine's critical infrastructure to evolving cyber threats.

This study contributes to the field by proposing an integrated model for protecting Ukraine's critical infrastructure, combining technological, organisational, and legal mechanisms tailored to address hybrid and evolving cyber threats. From a logistics systems perspective, the study shows how the cyber-resilience of energy, transport, financial, and governmental infrastructure supports continuity of operations, crisis response, resource allocation, and military readiness. The remainder of the article presents the materials and methods, analyses sector-specific vulnerabilities and protection mechanisms, discusses the findings in relation to the literature, and concludes with the study's limitations and directions for further research.

Materials and Methods

The study employed a qualitative multi-stage research design combining case study analysis, comparative legal analysis, and the synthesis of technical, organisational, and regulatory protection mechanisms. The research procedure involved identifying relevant cyber incidents, regulatory documents, cybersecurity standards, and scholarly publications; classifying the selected materials according to the affected critical infrastructure sector, type of cyber threat, identified vulnerability, protective measure, and institutional or legal response; comparing the Ukrainian findings with international cybersecurity standards and cooperation mechanisms; and synthesising the results of the technical, organisational, and legal analyses into an integrated cybersecurity model for Ukraine's critical infrastructure.

The cases were selected according to the following criteria: their direct relevance to Ukraine's critical infrastructure; documented consequences for essential services, public administration, or national security; representation of different forms of cyber threat, including state-sponsored, hybrid, espionage, and information operations; availability of verifiable open-source documentation; and suitability for analysing the interaction between technical vulnerabilities, organisational response, and legal regulation. Cases lacking sufficient documentary evidence or having no direct connection with critical infrastructure protection were excluded.

The analytical procedure involves a multi-step approach: first, a systematic classification of sector-specific vulnerabilities and threats, followed by an evaluation of existing technological, organisational, and legal mechanisms through comparative analysis with international standards. The evidential basis for the proposed model includes case study data, legal frameworks, national cybersecurity strategies, and technological solutions such as AI-based monitoring systems, the Zero Trust Model, and quantum cryptography, which are evaluated for their effectiveness in mitigating identified risks. The assessment applied adapted national cybersecurity standards (Ukrainian Research and Training Centre of Standardization, Certification and Quality 2023), the NIST framework (2024), CERT-UA (2025), National Council of ISACs (2025), national legislation, and the Budapest Convention on Cybercrime (2001).

The proposed model was validated analytically through methodological triangulation. Its components were cross-checked against three evidence groups: documented vulnerabilities and consequences identified in the selected Ukrainian cases; requirements and functions established in national legislation and international standards; and protective mechanisms discussed in the relevant scholarly literature. Internal consistency was assessed by determining whether each identified vulnerability was linked to an appropriate technical, organisational, or legal response and whether the proposed components corresponded to the functions of prevention, detection, response, recovery, and continuous improvement.

Results
Theoretical and methodological foundations of cybersecurity in Ukraine

Ukraine's critical infrastructure includes interconnected energy, transport, financial, governmental, telecommunications, healthcare, and public utility systems essential to national security and economic stability. Their growing reliance on supervisory control and data acquisition / industrial control systems (SCADA/ICS), corporate networks, and monitoring platforms improves efficiency but also increases exposure to cyberattacks with physical, economic, and social consequences. To address RQ1, Table 1 maps the principal sectors of Ukraine's critical infrastructure, their cyber components, and the potential threats affecting them.

Table 1. Classification of Ukraine's critical infrastructure, its cyber components, and examples of potential threats

Critical infrastructure sector	Main facilities	Cyber components	Examples of potential threats
Energy	Power plants, substations, power grids	SCADA/ICS, monitoring systems, corporate networks	Cyberattacks targeting energy generation and distribution management, system shutdowns
Transport	Airports, railways, logistics systems	enterprise resource planning (ERP) systems, traffic control systems, communication networks	Interference with routing, disruption of transport safety
Finance	Banks, payment systems	Online banking, corporate networks, databases	Theft of financial data, fraudulent transactions
Public administration	Government networks, e-governance systems	Unified state registries, document management, public service portals	Unauthorised access, breaches of registration systems
Healthcare	Hospitals, laboratories	Medical information systems, patient databases	Breach of electronic medical records, disruption of life-support systems

Source: compiled by the authors based on Gerasimenko (2024)

The nature of cyber threats to Ukraine is shaped by a combination of global trends and the specific regional context, including ongoing hybrid aggression. Ukraine's critical infrastructure faces state-sponsored operations and large-scale cyberattacks targeting energy, transport, government systems, strategic data, and public decision-making through espionage, social engineering, and disinformation. To further address RQ1, Table 2 classifies the principal cyber threats affecting

Ukraine according to their origin, operational characteristics, and documented manifestations.

Table 2. Classification of cyber threats specific to Ukraine

Threat type	Description	Examples
State-sponsored cyber operations	Attacks on strategic government and defence systems	2015-2016 power grid attacks; intrusions into government networks
Hybrid and military cyber operations	Complex actions combining physical impact and cyber tools	Attacks on energy substations during the 2022 military aggression
Cyber espionage and economic cyber activity	Unauthorised collection of strategic information	Theft of banking data, intellectual property
Disinformation campaigns and social engineering	Manipulation of public opinion and organisational decision-making	Mass phishing campaigns, attacks on government portals with disinformation

Source: compiled by the authors based on BBC News Ukrainian (2017), Office of the United Nations High Commissioner for Human Rights (2024), Burdiak (2024), Ilyenko et al. (2025)

The main tendencies in cybersecurity threats to Ukraine's critical infrastructure are characterised by state-sponsored cyber operations targeting key sectors like energy and government institutions, often aiming to both disrupt services and exploit vulnerabilities for future attacks. Hybrid and military cyber operations complicate the situation by combining cyberattacks with physical military actions, amplifying the scale of destruction. Cyber espionage and economic cyber activities also pose significant risks, undermining national security by targeting sensitive financial and intellectual data. Additionally, disinformation campaigns and social engineering are increasingly used to manipulate public perception and destabilise societal trust. These trends highlight systemic vulnerabilities, necessitating a multifaceted cybersecurity approach that integrates technological, organisational, and legal measures for enhanced protection.

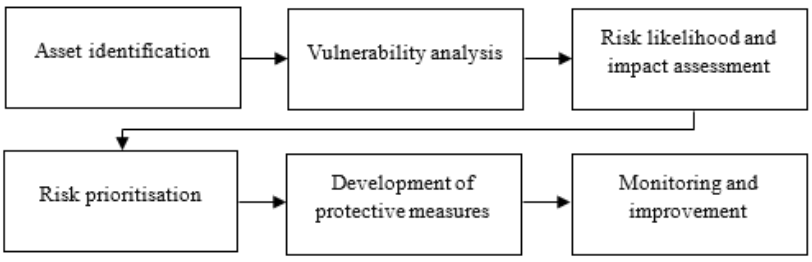


Figure 1. Cyber risk assessment model for Ukraine's critical infrastructure
Source: compiled by the authors based on Chehri et al. (2021)

Figure 1 operationalises the analysis undertaken for RQ1 by presenting the sequence used to identify and prioritise cyber risks, while also providing the risk-assessment basis for the integrated model examined in RQ4.

At the technical analysis level, systematic methods are applied, including vulnerability assessment, penetration testing, and cyberattack scenario modelling to identify potential paths of system compromise. For the organisational assessment of risks, adapted national cybersecurity standards are applied, including Ukrainian Research and Training Centre of Standardization, Certification and Quality (2023) and an adaptation of the international framework of NIST (2024), which enable the identification and ranking of risks based on their likelihood of occurrence and potential impact on the functioning of critical infrastructure. Scenario planning is also a priority in cyber risk assessment and management, modelling the development of incidents within intersectoral interdependencies and providing a foundation for the design of emergency response strategies.

Technological solutions for the cyber protection of Ukraine's critical infrastructure

Ukraine's critical infrastructure cybersecurity relies on multilayered architectural, infrastructural, and technological solutions, which Table 3 compares across sectors in relation to RQ3.

Table 3. Architectural and technological solutions for the cyber protection of Ukraine's critical infrastructure

Sector	Key protective technologies	Infrastructural approaches	Implementation features in Ukraine
Energy	Segmented SCADA/ICS, data encryption, disaster recovery systems	Isolation of critical nodes, backup lines, secure gateways	Centralised management of power networks, integration with CERT-UA
Transport	ERP platforms, IoT sensors, network gateways, traffic monitoring systems	Segmented networks, VPN, role-based access control	Applied in railway and airport systems, local data processing
Finance	Multi-factor authentication, behavioural analysis systems, intrusion detection and prevention systems (IDS/IPS)	Centralised data centres, database encryption	Collaboration between banks and state regulators for anomaly detection
Government systems	Secure cloud platforms, role-based access control, cryptographic tools	Isolated internal networks, centralised control points	Connection of electronic registries, integration with national cybersecurity platforms

Source: compiled by the authors based on NIST (2024), Maglaras et al. (2022)

The Ukrainian context is distinguished by close collaboration between banking institutions and state regulators, enabling more effective real-time detection and blocking of anomalies. In government systems, priorities include secure cloud solutions, strict access control, and the use of advanced cryptographic mechanisms. Internal network isolation and centralised control points create a secure environment for critical electronic registries and government platforms. A key factor is the integration of these solutions with the national cybersecurity infrastructure, ensuring alignment with the state's strategic objectives.

Table 4 extends the analysis of RQ3 and supports RQ4 by showing how detection, mitigation, information-sharing, and incident-response systems can be integrated into a coordinated cybersecurity ecosystem.

Table 4. Systems for detection, mitigation and response to cyber incidents in Ukraine

System type	Core functions	Examples in Ukraine	Level of integration
Response centres (CERT-UA)	Monitoring, response coordination, incident analysis	National CERT, regional units	High; coordination between the state and private sectors
Anomaly detection platforms	Traffic analysis, IDS/IPS, attack forecasting	SIEM systems, machine learning platforms	Integrated across energy, transport, and banking sectors
Network gateways and isolation systems	Filtering, network segmentation, access control	Secured SCADA/ICS gateways, VPNs	Used to isolate critical nodes and communications
Information hubs (ISACs)	Threat information sharing, collective response	ISACs for the energy and finance sectors	Supports national cybersecurity coordination

Source: compiled by the authors based on NIST (2024), CERT-UA (2025), Knapp (2024)

As shown in Figure 2, Ukraine's strategic assets are protected through integrated access control, network monitoring, encryption, data backup, network isolation, centralised communication control, staff training, and standardised incident-response protocols.

Network segmentation, IDS/IPS, the Zero Trust Model, AI-based monitoring, risk assessment, CERT-UA and ISAC coordination, and continuous improvement mechanisms are drawn from established standards, institutional practices, and existing cybersecurity research. The authors' contribution lies in integrating these elements into a unified model tailored to Ukraine's critical infrastructure, linking sector-specific vulnerabilities with technical protection, organisational coordination, legal responsibilities, incident response, and adaptive improvement.

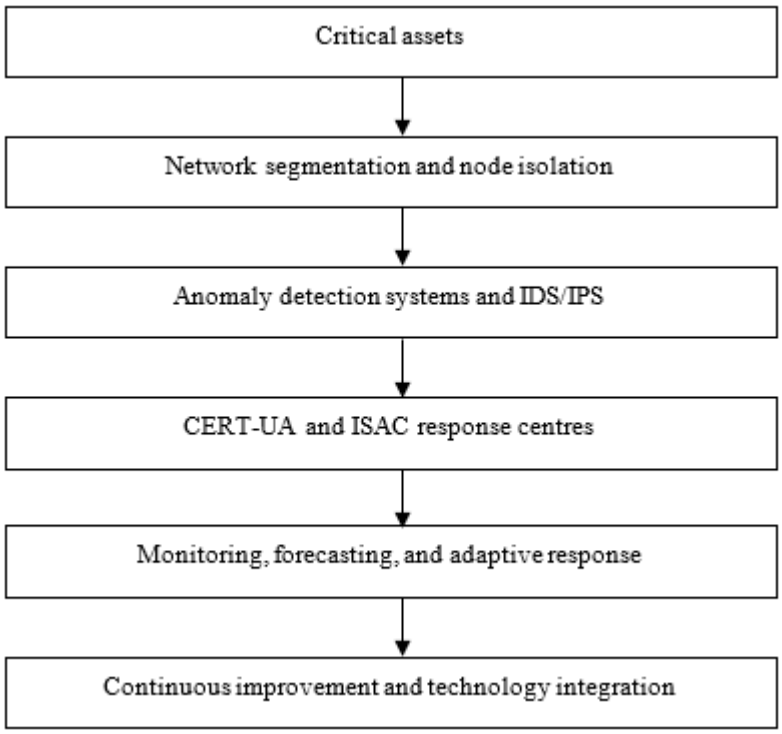


Figure 2. Integrated cybersecurity model for Ukraine's critical infrastructure
Source: compiled by the authors based on NIST (2024), CERT-UA (2025), and the findings of the present study

Legal and regulatory framework for cybersecurity in Ukraine

To address RQ2, Table 5 systematises the national legislation and strategic documents governing cybersecurity and critical infrastructure protection in Ukraine (Table 5).

Ukraine's status as a candidate for European Union membership has made approximation to the acquis communautaire an important component of critical infrastructure reform. Directive (EU) 2022/2557 (2022) establishes an all-hazards framework for strengthening the resilience of critical entities, including the adoption of national strategies, regular risk assessments, the identification of critical entities, resilience measures, incident notification, and coordination between competent authorities. Ukraine's initial self-screening (Report on the Initial Assessment... 2023)

identified amendments to the Law of Ukraine No. 1882-IX 'On Critical Infrastructure' (2021) as a priority measure for implementing the Directive. According to the European Commission's Ukraine 2025 Report (2025), the Ukrainian legal framework concerning critical infrastructure protection and the resilience of critical entities is partially aligned with the EU acquis, although resilience-related provisions have already been incorporated into national legislation to a significant extent.

Table 5. Key legislative acts and strategic documents of Ukraine in the field of cybersecurity

Law/Document	Year adopted	Main content	Key provisions	Notes on application
Law No. 2163-VIII	2017	Establishes the foundations of national cybersecurity policy	Cybersecurity actors, national cybersecurity system, powers of state authorities	Foundational document for the development of the national cybersecurity system
Cybersecurity Strategy of Ukraine, approved by Presidential Decree No. 447/2021	2021	Sets the direction for cybersecurity development over 5-10 years	Enhancing critical infrastructure resilience, integration of international practices	Updates approaches, reflecting previous experience and international standards
Law of Ukraine No. 4336-IX	2025	Strengthens the accountability of state authorities and critical infrastructure operators	Introduction of designated cybersecurity positions, unified incident response system	Ensures coordination between the public and private sectors in incident response

Source: compiled by the authors based on Law of Ukraine No. 2163-VIII 'On the Basic Principles of Cybersecurity in Ukraine' (2017), Cybersecurity Strategy of Ukraine, approved by Presidential Decree No. 447/2021 (2021), Law of Ukraine No. 4336-IX 'On Amendments to Certain Laws of Ukraine on Information Protection and Cyber Protection of State Information Resources and Critical Information Infrastructure Facilities' (2025)

Systematic alignment with international standards is an integral component of Ukraine's legal framework. Ukraine is a party to the Council of Europe Convention on Cybercrime, opened for signature in Budapest in 2001, which provides the legal basis for criminalising specific types of cybercrime and facilitates international cooperation in combating them. At the global level, this framework is complemented by the United Nations Convention against Cybercrime (2024). The Convention strengthens international cooperation in preventing and combating cybercrime and facilitates the collection, preservation, and sharing of electronic evidence relating to serious crimes. Furthermore, cooperation with NATO and the EU enables the integration of best practices in cybersecurity, the conduct of joint exercises and training, and the real-time exchange of information on cyber threats. As a result, Ukraine's national cybersecurity system is being developed as a multi-layered structure, where technical, organisational, and regulatory components interact to provide comprehensive protection of strategically important assets. Table 6 further

develops RQ2 by clarifying the distribution of cybersecurity responsibilities and coordination mechanisms among public authorities and private-sector operators.

Table 6. Key cybersecurity actors in Ukraine and their powers

Actor	Role in cybersecurity	Key powers	Interaction with other actors	Principal legal, strategic and policy instruments
National Security and Defence Council of Ukraine	Strategic leadership	Determination of strategic policy directions; approval of plans	Coordinates the activities of all state authorities	Law of Ukraine No. 183/98-VR 'On the National Security and Defence Council of Ukraine' (1998); Law of Ukraine No. 2469-VIII 'On National Security of Ukraine' (2018); Cybersecurity Strategy of Ukraine, approved by Presidential Decree No. 447/2021 (2021).
State Service of Special Communications and Information Protection of Ukraine	Implementation of state policy	Protection of information; oversight of legal compliance; cybersecurity audits	Interacts with central government authorities and critical infrastructure	Law of Ukraine No. 2163VIII 'On the Basic Principles of Cybersecurity in Ukraine' (2017); Law of Ukraine No. 3475-IV 'On the State Service for Special Communications and Information Protection of Ukraine' (2006); Resolution of the Cabinet of Ministers of Ukraine on the Procedure for Information Protection (2025)
Security Service of Ukraine	Counterintelligence	Prevention of cyberattacks; investigation of incidents	Collaboration with the private sector and international organisations	Law of Ukraine No. 2229-XII 'On Security Service of Ukraine' (1992); Council of Europe Convention on Cybercrime (2001)
Private sector	Compliance with regulatory requirements; protection of own systems	Response to cyber incidents; implementation of technical and organisational measures	Information exchange with CERT-UA and ISACs; coordination with state authorities	Law of Ukraine No. 4336-IX 'On Amendments to Certain Laws of Ukraine on Information Protection and Cyber Protection of State Information Resources and Critical Information Infrastructure Facilities' (2025); NIST (2024)

Source: compiled by the authors

Ukraine's national cyber-resilience system is based on coordinated action among the National Security and Defence Council, which defines strategic priorities; the State Service of Special Communications and Information Protection, which implements policy and ensures technical compliance; the Security Service of Ukraine,

which prevents and investigates cyberattacks; and critical infrastructure operators and private-sector organisations protecting their systems and cooperating with CERT-UA, sector-specific ISACs, and international partners.

Challenges and strategic directions for the development of Ukrainian cybersecurity

Ukraine's contemporary cyberspace is characterised by a high level of threat dynamism, reflecting the nature of hybrid warfare and emphasising the need for a comprehensive cybersecurity system. Analysis of current cyber threats shows that Ukraine faces a wide range of attacks: from large-scale DDoS and phishing campaigns to targeted assaults on critical infrastructure, including energy, transport, financial, and government information systems. Table 7 illustrates key vulnerabilities and the protective measures implemented across sectors.

Table 7. Vulnerable sectors of Ukraine's critical infrastructure and protective measures

Sector	Vulnerabilities	Implemented protective measures
Energy	Insufficient protection of automated control systems; lack of redundant communication channels	Implementation of monitoring and incident response systems; redundancy for critical components
Transport	Outdated software; absence of centralised oversight	Software updates; centralised management
Healthcare	Lack of data encryption; insufficient access control	Data encryption; multi-factor authentication
Finance	Weak protection of payment systems; vulnerabilities in mobile applications	Additional security layers; security audits

Source: compiled by the authors based on Tarasenko et al. (2022)

In the context of cybersecurity development, a key priority is hardware-level protection, which includes installing physical access control devices and anomaly detection on IoT devices – measures that are especially crucial for energy, transport, and government systems. Table 8 summarises the strategic directions for cybersecurity development, highlighting key technologies and their practical applications.

Table 8. Key directions for cybersecurity development in Ukraine

Development direction	Description	Example of application
Hardware-level protection	Securing IoT devices through physical measures	Implementation of secure chips in devices to prevent unauthorised access
Zero Trust Model	Verification of every user and device at every access point	Multi-factor authentication and behavioural monitoring of users
AI-driven monitoring and protection	Analysis of network traffic, anomaly detection, automated response	AI-based systems for real-time detection and blocking of cyber threats
Quantum cryptography	Use of quantum-resistant algorithms and quantum key distribution	Development and implementation of encryption standards to safeguard data

Source: compiled by the authors based on Tarasenko et al. (2022)

Discussion

The findings of this study have significant implications for Ukraine's logistics systems, continuity of operations, crisis response, and military security. The integration of multi-layered cybersecurity protection across critical sectors, including energy, transport, and finance, is crucial to maintaining the stability of logistics networks and ensuring the uninterrupted flow of essential services. The implementation of advanced technologies, such as AI-based monitoring and the Zero Trust Model, enhances the resilience of these systems, enabling rapid detection and mitigation of cyber threats. This, in turn, supports crisis response by enabling timely decision-making and resource allocation during disruptions. Moreover, the security of critical infrastructure is closely tied to national military security, as cyberattacks on logistics and government systems can have direct consequences on military operations. By strengthening cybersecurity measures, Ukraine can enhance its overall resilience, reduce vulnerabilities in military and civilian operations, and better manage the complex interdependencies between various sectors in times of crisis.

Klenka (2021) examines the legal aspects of aviation cybersecurity, emphasising the need to integrate regulatory and organisational measures into an overall protection system. Compared with the present study, which focuses on the technical, organisational, and regulatory mechanisms for protecting Ukraine's critical infrastructure (energy, transport, finance, government systems, and healthcare), Klenka's publication is primarily concerned with legal and regulatory aspects, whereas the current research provides a comprehensive assessment of information system vulnerabilities and practical protective measures.

Rakha (2023) investigates the legal aspects of ensuring cybersecurity for remote workforces and examines international best practices, emphasising the role of regulatory frameworks and corporate policies in risk mitigation. Compared with the present study, which focuses primarily on the technical, organisational, and regulatory mechanisms for protecting Ukraine's critical infrastructure, Rakha's publication centres on remote access and flexible working arrangements. While these considerations are less relevant for sectors with a high concentration of SCADA/ICS and ERP systems, they complement the understanding of socio-technical aspects of cyber risks.

Tsantikidou and Sklavos (2024) emphasise cryptographic protection of critical infrastructure, which corresponds with the present study's focus on quantum cryptography and multi-level encryption, although this study also integrates organisational and regulatory measures. Similarly, Rees and Rees (2023) highlight state and non-state threats and the need for cross-sector coordination, supporting the proposed integration of CERT-UA, sector-specific ISACs, and incident-response systems, while the current research further adapts these mechanisms to Ukraine's legal, institutional, and risk-management context.

The analysis of political and regulatory aspects in the study of Atkins and Lawson (2021) indicates that fragmented state policies often result in gaps in the protection of critical infrastructure and delayed threat response. This aligns with the current findings emphasising the importance of integrating technical, organisational, and regulatory measures to enhance protection effectiveness. However, the Ukrainian system is still in the process of adapting international practices.

The review of scholarly sources in the comparison with this study reveals strong alignment in technical and organisational strategies, though discrepancies arise due to Ukraine's specific regulatory development, governance, and the need to adapt international practices locally.

Conclusions

The study examines Ukraine's cybersecurity framework, highlighting that critical infrastructure encompasses both physical assets and their supporting information systems. It identifies hybrid and targeted cyber threats, including those involving advanced technologies such as AI and automated botnets. The country's cyber-risk assessment methods can identify critical vulnerabilities but need constant updates to address emerging threats. Infrastructure analysis reveals that Ukraine's energy, transport, finance, and government sectors are gradually adopting multi-layered protection strategies, combining physical, software, and organisational components. Detection and response systems have been effective in localising threats and

mitigating their impact on critical processes. The integration of AI-based systems and Zero Trust Models strengthens the resilience of strategic assets and prepares for large-scale automation of defence processes. Legislative developments show that Ukraine's regulatory framework is adapting to dynamic cyber threats, facilitating coordination between public and private sectors. Despite these advancements, Ukraine remains a target for hybrid attacks combining technical, informational, and physical methods. Vulnerabilities in automated control systems, outdated software, limited access control, and lack of backup communication channels have been identified. The use of advanced technologies, such as AI, Zero Trust, and quantum cryptography, within a comprehensive cyber-resilience framework, can significantly reduce risks and enhance system adaptability.

Taken together, the findings answer RQ1–RQ4 by identifying inadequate protection of automated control systems, outdated software, limited access control, and insufficient backup communications as the principal vulnerabilities; showing that the regulatory framework is developing but still requires stronger public–private coordination and alignment with international standards; indicating that AI-based monitoring, the Zero Trust Model, and quantum cryptography may strengthen resilience; and suggesting that an integrated combination of technical, organisational, and legal measures can improve readiness for hybrid cyber threats. These findings support the study hypothesis at an analytical level, although the operational effectiveness of the proposed model requires empirical validation. The scientific contribution lies in integrating these dimensions within a model tailored to Ukraine. For logistics systems, the practical implication is improved continuity of supply, transport operations, information flows, crisis resource allocation, and military readiness.

The study is limited to an analysis of the primary sectors of Ukraine's critical infrastructure and open-source incident data, which may not fully reflect the security status of all facilities. Future research should expand coverage to include private and less critical assets, integrate additional threat prediction methods using artificial intelligence and big data, and undertake a more detailed comparison of Ukrainian practices with a broader range of international standards and regional approaches.

References

Atkins, S. and Lawson, C., 2021. An improvised patchwork: success and failure in cybersecurity policy for critical infrastructure. *Public Administration Review*, 81(5), 847–861. DOI: 10.1111/puar.13322.

BBC News Ukrainian, 2017. The power outage in Ukraine was a hacker attack [online]. Available from: https://www.bbc.com/ukrainian/news-38585587 [Accessed: 19 December 2025].

Bechara, F.R. and Schuch, S.B., 2021. Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, 28(2), 359–374. DOI: 10.1108/JFC-07-2020-0149.

Burdiak, P., 2024. *A malicious alliance: how cyberattacks and disinformation are synchro-*

nously destabilizing the digital space of Ukraine in the face of Russian aggression. Kyiv: Center for Democracy and Rule of Law. Available from: https://cedem.org.ua/wp-content/uploads/2024/12/CEDEM_cyberdis_eng.pdf [Accessed: 15 December 2025].

Cabinet of Ministers of Ukraine, 2023. *Report on the initial assessment of the progress in the implementation of the European Union legal acts (EU acquis)*. Kyiv: Cabinet of Ministers of Ukraine. Available from: https://eu-ua.kmu.gov.ua/wp-content/uploads/Zvit_EN.pdf [Accessed: 10 June 2026].

Cabinet of Ministers of Ukraine, 2025. Resolution No. 712 of 18 June 2025 'Some issues of protection of information, electronic communications, information and communication systems and technological systems'. Available from: https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF#Text [Accessed: 14 July 2026].

CERT-UA, 2025. CERT-UA [online]. Available from: https://cert.gov.ua/ [Accessed: 17 December 2025].

Chehri, A., Fofana, I., and Yang, X., 2021. Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence. *Sustainability*, 13(6), 3196. DOI: 10.3390/su13063196.

Council of Europe, 2001. Convention on Cybercrime (ETS No. 185). Available from: https://www.coe.int/en/web/cybercrime/the-budapest-convention [Accessed: 11 December 2025].

Cybersecurity Strategy of Ukraine, approved by Presidential Decree No. 447/2021 [online], 2021. Available from: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf [Accessed: 23 December 2025].

European Commission, 2025. *Ukraine 2025 report*. Brussels: European Commission, SWD(2025) 759 final. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025SC0759 [Accessed: 10 June 2026].

European Parliament and Council of the European Union, 2022. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. *Official Journal of the European Union*, L 333, 164–198. Available from: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng [Accessed: 10 June 2026].

Gerasimenko, O.M., 2024. Threats to critical infrastructure facilities in Ukraine under martial law. *Scientific Bulletin of Uzhhorod National University. Series: Law*, 3(84), 257–263. DOI: 10.24144/2307-3322.2024.84.3.39.

Ilyenko, A., Teliushchenko, V., and Dubchak, O., 2025. Modern cyber threats to critical infrastructure in Ukraine and the world. *Cybersecurity: Education, Science, Technique*, 3(27), 150–164. DOI: 10.28925/2663-4023.2023.27.719.

Klenka, M., 2021. Aviation cyber security: legal aspects of cyber threats. *Journal of Transportation Security*, 14(3), 177–195. DOI: 10.1007/s12198-021-00232-8.

Knapp, E.D., 2024. *Industrial network security: securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems*. 3rd ed. Cambridge, MA: Syngress. DOI: 10.1016/C2022-0-02315-1.

Kumar, A., 2024. Examining cybersecurity laws: protecting critical infrastructure against emerging threats and global cybercrimes. *Journal of Law and Intellectual Property Rights*, 1(1), 21–29. Available from: https://jlipr.in/doc/Vol-1-No-1-2024/3_JLIPR_Vol%201%20%20No%201_Dec%202024.pdf [Accessed 15 December 2025].

Law of Ukraine No. 183/98-VR of 5 March 1998 'On the National Security and Defence Council of Ukraine', 1998. Available from: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text [Accessed: 14 July 2026].

Law of Ukraine No. 1882-IX of 16 November 2021 'On Critical Infrastructure', 2021. Avail-

able from: https://zakon.rada.gov.ua/laws/show/1882-20#Text [Accessed: 14 July 2026].

Law of Ukraine No. 2163-VIII of 5 October 2017 'On the Basic Principles of Cybersecurity in Ukraine', 2017. Available from: https://zakon.rada.gov.ua/laws/show/2163-19#Text [Accessed: 14 July 2026].

Law of Ukraine No. 2229-XII of 25 March 1992 'On Security Service of Ukraine', 1992. Available from: https://zakon.rada.gov.ua/laws/show/2229-12#Text [Accessed: 14 July 2026].

Law of Ukraine No. 2469-VIII of 21 June 2018 'On National Security of Ukraine', 2018. Available from: https://zakon.rada.gov.ua/laws/show/2469-19#Text [Accessed: 14 July 2026].

Law of Ukraine No. 3475-IV of 23 February 2006 'On the State Service for Special Communications and Information Protection of Ukraine', 2006. Available from: https://zakon.rada.gov.ua/laws/show/3475-15#Text [Accessed: 14 July 2026].

Law of Ukraine No. 4336-IX of 27 March 2025 'On Amendments to Certain Laws of Ukraine on Information Protection and Cyber Protection of State Information Resources and Critical Information Infrastructure Facilities', 2025. Available from: https://zakon.rada.gov.ua/laws/show/4336-20#Text [Accessed: 14 July 2026].

Lehto, M., 2022. Cyber-attacks against critical infrastructure. In: M. Lehto and P. Neittaanmäki, eds. *Cyber security: critical infrastructure protection*. Cham: Springer, 3–42. DOI: 10.1007/978-3-030-91293-2_1.

Maglaras, L., Janicke, H., and Ferrag, M.A., 2022. Cybersecurity of critical infrastructures: challenges and solutions. *Sensors*, 22(14), 5105. DOI: 10.3390/s22145105.

Malatji, M., Marnewick, A.L., and Von Solms, S., 2022. Cybersecurity capabilities for critical infrastructure resilience. *Information and Computer Security*, 30(2), 255–279. DOI: 10.1108/ICS-06-2021-0091.

National Council of ISACs, 2025. National Council of ISACs [online]. Available from: https://www.nationalisacs.org/ [Accessed: 10 December 2025].

National Institute of Standards and Technology, 2024. *The NIST Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD: National Institute of Standards and Technology, NIST CSWP 29. DOI: 10.6028/NIST.CSWP.29.

Office of the United Nations High Commissioner for Human Rights, 2024. *Attacks on Ukraine's energy infrastructure: harm to the civilian population*. Kyiv: United Nations Human Rights Monitoring Mission in Ukraine. Available from: https://ukraine.ohchr.org/sites/default/files/2024-12/UKR_Attacks_on_Ukraine%E2%80%99s_Energy_Infrastructure_Harm_to_the_Civilian.pdf [Accessed: 12 December 2025].

Onyshchenko, S. and Hlushko, A., 2022. Analytical dimension of cybersecurity of Ukraine in the conditions of growing challenges and threats. *Economics and Region*, 1(84), 13–20. DOI: 10.26906/EiR.2022.1(84).2540.

Rakha, N.A., 2023. Ensuring cyber-security in remote workforce: legal implications and international best practices. *International Journal of Law and Policy*, 1(3), 1–19. DOI: 10.59022/ijlp.43.

Rees, J. and Rees, C.J., 2023. Cyber-security and the changing landscape of critical national infrastructure: state and non-state cyber-attacks on organisations, systems and services. In: R. Montasari, ed. *Applications for artificial intelligence and digital forensics in national security*. Cham: Springer, 67–89. DOI: 10.1007/978-3-031-40118-3_5.

Tarasenko, O., et al., 2022. Cyber security as the basis for the national security of Ukraine. *Cuestiones Políticas*, 40(73), 583–599. DOI: 10.46398/cuestpol.4073.33.

Tsantikidou, K. and Sklavos, N., 2024. Threats, attacks, and cryptography frameworks of cybersecurity in critical infrastructures. *Cryptography*, 8(1), 7. DOI: 10.3390/cryp-

tography8010007.
Ukrainian Research and Training Centre of Standardization, Certification and Quality, 2023. *DSTU ISO/IEC 27005:2023 Information security, cybersecurity and privacy protection: guidance on managing information security risks (ISO/IEC 27005:2022, IDT)*. Kyiv: Ukrainian Research and Training Centre of Standardization, Certification and Quality. Available from: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104400 [Accessed: 14 December 2025].
United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes. Resolution 79/243, adopted on 24 December 2024. [online], 2024. Available from: https://docs.un.org/en/a/res/79/243 [Accessed: 10 June 2026]
Watney, M., 2022. Cybersecurity threats to and cyberattacks on critical infrastructure: a legal perspective. *Proceedings of the 21st European Conference on Cyber Warfare and Security*, 21(1), 319–327. DOI: 10.34190/eccws.21.1.196.

Author Contributions
Conceptualisation: OS, IM; Methodology: IM, MS; Formal analysis: OS, ML; Investigation: MS, ML; Data curation: OL, OS; Writing – original draft: IM, OL; Writing – review & editing: ML, IM; Visualisation: ML, OL; Supervision: OS; Project administration: OS.

Funding
This research received no external funding.

Data Availability Statement
Data are available from the corresponding author upon reasonable request.

Conflict of Interest Statement
The authors declare no conflict of interest.

Use of AI Tools
The authors did not use generative AI tools in preparing this manuscript.

Ethics Approval / Consent
Not applicable.

Acknowledgements
None.

Received: 14.04.2026
Accepted: 24.10.2026

© Oleh Semenenko, Ihor Mylashenko, Maryna Sliusarenko, Mykola Linevych, Oleksandr Leonenko, 2026. This article is published in "*Systemy Logistyczne Wojsk*" / *"Military Logistics Systems*" under the Creative Commons Attribution 4.0 International licence (CC BY 4.0).