OBSERVARE
Universidade Autónoma de Lisboa
e-ISSN: 1647-7251
VOL. 16, Nº. 2, TD3
Thematic Dossier
Rule of Law, Human Rights, and Institutional Transformation in Times of Global and National Challenges
March 2026

JANUS.NET
e-journal of International Relations

THE IMPORTANCE OF CRITICAL INFRASTRUCTURE FOR NATIONAL SECURITY: LEGAL ASPECTS, RISK MODELS AND MECHANISMS OF STATE MANAGEMENT OF SECURITY

SERHII BIELAI
belwz3@ukr.net
Doctor of Science in Public Administration, Professor Deputy Head of the Educational and Scientific Center for the Organization of the Educational Process Head of the Scientific and Methodological Department, National Academy of the National Guard of Ukraine
Kharkiv (Ukraine) https://orcid.org/0000-0002-0841-9522

OLEKSANDR PIVNENKO
halk.enemigo@gmail.com
National Guard of Ukraine Commander Main Headquarters of the National Guard of Ukraine
Kyiv (Ukraine) https://orcid.org/0009-0009-3528-609X

VADYM YEVSIEIEV
ua117@ukr.net
PhD in Military Sciences, Associate Professor, Head of the Center Retraining and Advanced Training Center, National Academy of the National Guard of Ukraine
Kharkiv (Ukraine) https://orcid.org/0000-0002-0164-2991

VADYM HLADKOV
vadimgs1806@gmail.com
First Deputy (Chief of Staff) of the Commander of the National Guard of Ukraine, Main Headquarters of the National Guard of Ukraine
Kyiv (Ukraine) https://orcid.org/0009-0001-3705-1974

IVAN LAVROV
johnapleased417@gmail.com
Postgraduate and Doctoral Studies, National Academy of the National Guard of Ukraine
Kharkiv (Ukraine) https://orcid.org/0009-0005-0706-3711

Abstract

In Ukraine, where the war creates additional challenges, the rapid restoration and adaptation of critical infrastructure form the basis of the national security field. Between February 2022 and the end of 2023, more than 1,200 major cyberattacks were recorded in Ukraine, approximately 40% of which were directed against energy and communication systems, and the damage from missile and drone strikes on infrastructure exceeded $137 billion. The purpose of this article is to analyze the functionality of legal support critical infrastructure in the national security system in the current context of military challenges. The study examines the structure of legal aspects, support critical infrastructure and its place in the overall security system of the state. Various risk assessment methods are analyzed, such as system models, multi-level models, and cybernetic models, which help predict possible crisis situations and plan measures to prevent or mitigate damage. It is argued that resilience can be enhanced through digital technologies, cybersecurity measures, legal reforms, and better coordination between public and private organizations. The prospects for optimizing the state of critical infrastructure in Ukraine are considered, including diversification of supply, modernization of the energy system, improvement of legislation in accordance with European requirements, and improvement of the investment climate. A generalized author's model for managing the

resilience of critical infrastructure in Ukraine during times of increased risk of war is proposed. The study emphasizes the importance of the legal aspects resilience of critical infrastructure, its ability to recover quickly, and highlights the role of cooperation between the public and private sectors.

Keywords

Critical infrastructure, national security, risks, resilience, international experience, legal aspects.

Resumo

Na Ucrânia, onde a guerra cria desafios adicionais, a rápida restauração e adaptação de infraestruturas críticas constituem a base do domínio da segurança nacional. Entre fevereiro de 2022 e o final de 2023, foram registados mais de 1200 ciberataques de grande dimensão na Ucrânia, dos quais aproximadamente 40% foram dirigidos contra sistemas energéticos e de comunicação, e os danos causados por ataques com mísseis e drones às infraestruturas excederam os 137 mil milhões de dólares. O objetivo deste artigo é analisar a funcionalidade do apoio jurídico às infraestruturas críticas no sistema de segurança nacional no contexto atual de desafios militares. O estudo examina a estrutura dos aspetos jurídicos, o apoio às infraestruturas críticas e o seu lugar no sistema geral de segurança do Estado. São analisados vários métodos de avaliação de riscos, tais como modelos de sistema, modelos multiníveis e modelos cibernéticos, que ajudam a prever possíveis situações de crise e a planear medidas para prevenir ou mitigar danos. Argumenta-se que a resiliência pode ser reforçada através de tecnologias digitais, medidas de cibersegurança, reformas jurídicas e uma melhor coordenação entre organizações públicas e privadas. São consideradas as perspetivas de otimização do estado das infraestruturas críticas na Ucrânia, incluindo a diversificação do abastecimento, a modernização do sistema energético, a melhoria da legislação em conformidade com os requisitos europeus e a melhoria do clima de investimento. É proposto um modelo generalizado do autor para gerir a resiliência das infraestruturas críticas na Ucrânia em tempos de risco acrescido de guerra. O estudo enfatiza a importância dos aspetos jurídicos da resiliência das infraestruturas críticas, a sua capacidade de recuperação rápida e destaca o papel da cooperação entre os setores público e privado.

Palavras-chave

Infraestruturas críticas, segurança nacional, riscos, resiliência, experiência internacional, aspetos jurídicos.

How to cite this article

Bielai, Serhii Pivnenko, Oleksandr, Yevsieiev, Vadym, Hladkov, Vadym & Lavrov, Ivan (2026). The Importance of Critical Infrastructure for National Security Risk Models and Mechanisms of State Management of Security. *Janus.net, e-journal of international relations*. Thematic Dossier - Rule of Law, Human Rights, and Institutional Transformation in Times of Global and National Challenges, VOL. 16, Nº. 2, TD3, March 2026, pp. 293-314. https://doi.org/10.26619/1647-7251.DT0226.16

Article submitted on 23 November 2025 and accepted for publication on 08 January 2026.

JANUS.NET, e-journal of International Relations
e-ISSN: 1647-7251
VOL. 16, Nº. 2, TD3
Thematic Dossier - *Rule of Law, Human Rights, and Institutional Transformation in Times of Global and National Challenges*
March 2026, pp. 293-314
The Importance of Critical Infrastructure for National Security Risk Models and Mechanisms of State Management of Security
Serhii Bielai, Oleksandr Pivnenko, Vadym Yevsieiev, Vadym Hladkov, Ivan Lavrov

THE IMPORTANCE OF CRITICAL INFRASTRUCTURE FOR NATIONAL SECURITY RISK MODELS AND MECHANISMS OF STATE MANAGEMENT OF SECURITY

SERHII BIELAI

OLEKSANDR PIVNENKO

VADYM YEVSIEIEV

VADYM HLADKOV

IVAN LAVROV

Introduction

Critical infrastructure, which includes energy, transportation, financial, information and communication systems, directly affects national security, as its failure or destruction can lead to serious consequences that threaten the sovereignty, territorial integrity and functioning of the state. The destruction of critical infrastructure causes uneven economic development, regional imbalance, outflow of financial and intellectual capital, growing social polarization, slowdown in innovation and investment, and increased environmental problems.

During the war in Ukraine, the risks of damage to critical infrastructure facilities are becoming alarming. According to the Business Ombudsman Council, more than 700 critical infrastructure facilities were damaged in 2022 alone. The government of Ukraine, together with the World Bank Group, the European Commission and the United Nations, published a report on an updated joint assessment of the damage and needs resulting from the large-scale invasion of Russia – Rapid Damage and Needs Assessment, RDNA3 (World Bank Group, 2024). The RDNA3 assessment covers the damage caused during the almost two-year period from the moment of Russia's full-scale invasion of Ukraine on February 24, 2022, to December 31, 2023. According to the report, direct losses in Ukraine have so far reached nearly $152 billion, with housing, transportation, trade and industry, energy, and agriculture identified as the most affected sectors. The destruction

of the Kakhovka hydroelectric dam in June 2023 led to catastrophic environmental consequences and exacerbated social problems.

Such challenges create a need for new approaches to legal support for public administration in the security sector, which must take into account the complex nature of threats to critical infrastructure and the need for rapid response. The aim of this work is to analyze the functionality of the legal aspects of critical infrastructure support in the national security system and to propose the author's concept for the formation of effective mechanisms for its protection in the conditions of martial law in Ukraine.

Literature Review

Scientists Obi et al. (2024), Ingvarson and Hassel (2023), as a result of their research on the multifactorial impact of critical infrastructure on the state of national security, identified the main vectors of such impact: resilience to threats (cyberattacks, physical destruction); recovery capacity; economic consequences (losses from damage to infrastructure and a long interruption in its functioning); societal life; defense capability dynamics; state stability, trust in the government and prevention of social conflicts. The researchers emphasize that it is important to take into account the cascading effect of threats, when the failure of one element affects the entire security system.

Lubis et al. (2025) explored the possibilities of quantifying the impact of critical infrastructure on national security and identified the main aspects of measurement, including quantifying damage and financial losses, vulnerability analysis (assessing the weaknesses of critical infrastructure that could potentially be affected), monitoring the functioning of systems to identify failures and their causes, and modeling the potential consequences of threats to critical infrastructure.

A number of scholars, in particular, Jada and Mayayise (2024), Saeed et al. (2023), emphasize the need to raise awareness of public sector employees about information security standards to prevent the risks of damage to critical infrastructure: ensuring the uninterrupted operation of facilities, preventing unauthorized interference, predicting crisis situations and preventing their negative impact. Furthermore, the scientists argue for the need to establish cooperation between the public sector, the public and business in the context of common interests in combating cyber threats, emphasizing the need for interagency coordination and public-private partnerships to improve system reliability.

Kalapodis et al. (2025) promote innovative IDS systems for detecting attack traffic, arguing that if more protection resources are invested in critical infrastructure, the ability to resist intrusions can be significantly higher.

Erbas et al. (2024), Paravantis and Kontoulis (2020), studying models for assessing risks and levels of impact on national security, concluded that the most effective assessment models for determining the likelihood of hazards and potential consequences (losses) from the realization of risks are statistical methods, expert assessments, simulation modeling, decision tree, sensitivity analysis, scenario analysis, as well as calculation and analytical and similar methods.

The publications of Eusgeld et al. (2011), Große (2021), Li et al. (2022) are considered relevant, where it is established that the protection of critical infrastructure includes activities to identify, prevent and neutralize threats, as well as minimize and eliminate the consequences of their implementation. The authors outline the boundaries of stakeholder responsibility in this context: the state determines the national policy in the field, forms legislative requirements and coordinates the work of the national critical infrastructure protection system; at the same time, owners (operators) are responsible for ensuring an adequate level of security of facilities, developing and implementing protection measures, as well as cyber defense.

Dimitropoulos (2020), Rass et al. (2020) proposed a number of methods for modeling security threats based on risk forecasting. The main approaches to threat modeling are as follows: threat modeling frameworks (e.g., TRIKE), including structured analysis and documentation of threats; analysis of risks and vulnerabilities, followed by an assessment of their consequences; prioritization of preventive countermeasures; development of a potential breach model to study and predict behavior, potential motives and methods of attacks.

Despite the significant scientific developments, the issue of rethinking the role of critical infrastructure in the national security system in wartime requires expanded research and the development of effective protection mechanisms.

Methodology

To achieve the stated research objective, a comprehensive methodological framework combining general scientific, special legal, and interdisciplinary methods was applied. This approach ensured a systematic and multifaceted analysis of the legal, organizational, and risk-related aspects of critical infrastructure protection within the national security system of Ukraine under wartime conditions.

The analytical method was used to systematize existing scientific approaches, international standards, and doctrinal positions concerning the role of critical infrastructure in ensuring national security. This method made it possible to identify key legal categories, regulatory gaps, and structural weaknesses in the current system of state management of critical infrastructure security.

The systemic and structural-functional methods were applied to examine critical infrastructure as an integrated element of the national security system, characterized by interdependence between energy, transport, communication, digital, and defense-related sectors. These methods allowed for the identification of functional links between legal regulation, institutional mechanisms, and practical security measures.

The comparative legal method was used to analyze Ukrainian legislation in the field of critical infrastructure protection in comparison with European Union legal acts, NATO resilience standards, and international best practices. This enabled the assessment of the level of harmonization of national legislation with European requirements and the identification of priority directions for legal adaptation.

The modeling method played a key role in assessing potential crisis scenarios and risks to critical infrastructure. System models, multi-level risk models, and cybernetic models were applied to simulate the impact of military, cyber, and hybrid threats, as well as to evaluate the resilience and recovery capacity of infrastructure systems under conditions of large-scale disruption.

The risk assessment and scenario analysis methods were employed to classify threats, determine their probability and potential consequences, and evaluate vulnerability levels across different infrastructure sectors. These methods supported the development of preventive and mitigation strategies aimed at enhancing infrastructure resilience.

The methods of synthesis and logical generalization were used to formulate an author's conceptual model of state management of critical infrastructure resilience during periods of heightened military risk. This model integrates legal regulation, cybersecurity measures, institutional coordination, and public–private partnership mechanisms.

In addition, content analysis of legal acts, strategic documents, and policy papers was conducted to identify prevailing regulatory approaches and emerging trends in critical infrastructure protection.

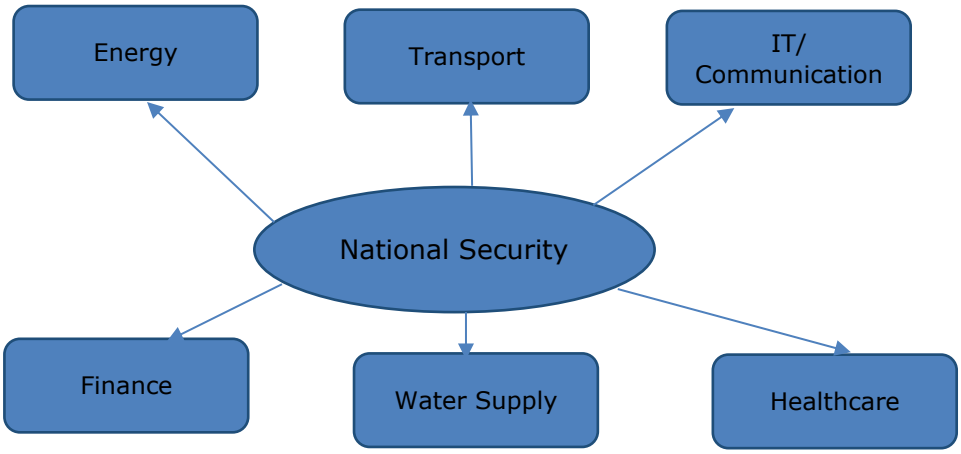
The limitations of the study are related to the restricted availability of classified data, the complexity of empirical verification of security models under wartime conditions, and potential regional bias due to uneven levels of infrastructure damage and restoration. Nevertheless, the applied methodological toolkit provides a sufficient basis for substantiated conclusions and practical recommendations aimed at strengthening the legal and institutional framework for critical infrastructure protection in Ukraine.

Results

Critical infrastructure is defined as a set of facilities, systems, and networks whose disruption has a significant impact on the security and stability of the state. It includes the energy sector, transportation systems, information and communication technologies, financial sector, and healthcare. In the scientific literature, the concept of "critical infrastructure" is interpreted as a multi-level system with a high degree of interdependence.

The full-scale war has shown the vulnerability of Ukraine's critical infrastructure and its direct impact on the overall security context on a national scale. From February 2022 to the end of 2023 alone, more than 63 thousand energy facilities were damaged, with total direct losses in the energy sector estimated at USD 8.8 billion. In the transport sector, more than 23.5 thousand kilometers of roads and more than 340 bridges were destroyed; in the healthcare sector, more than 1.5 thousand institutions were affected**,** 204 of which were completely destroyed; in cyberspace, more than 4.3 thousand incidents were recorded in 2024 alone (State Statistics Service of Ukraine, 2024). As of 2025, the intensity of threats to critical infrastructure continues to grow, with hybrid attacks affecting various areas gaining particular popularity (Figure 1) (Ilyenko et al., 2025).

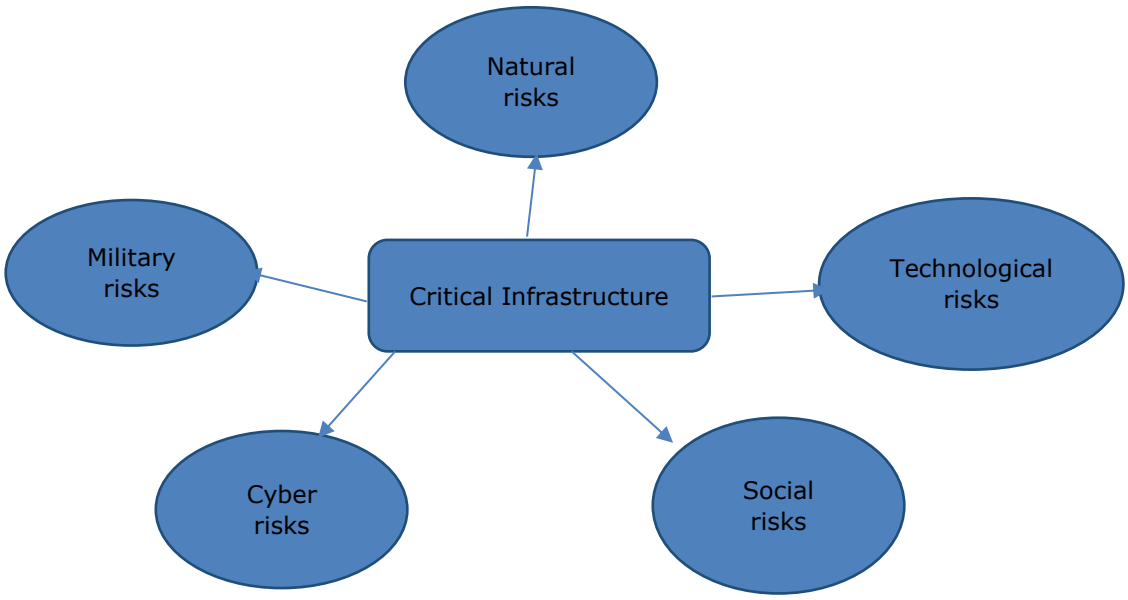
Figure 1. National security and critical infrastructure



Source: (Ilyenko et al., 2025)

Each element of the national security system performs a unique function, and the vulnerability of one segment can create a cascading effect (Novotny & Janosikova, 2020; Roshanaei, 2021). At the same time, cyberspace risks are of particular importance, along with other categories of critical infrastructure risks (Figure 2).

Figure 2. Risks of Critical Infrastructure



Source: created by the author based on Tzavara and Vassiliadis (2024)

The information in Figure 2 emphasizes the multidimensional nature of the risks of critical infrastructure destruction and highlights the urgent need to improve mechanisms for its protection, as economic stability, defense capability, and the level of social stability are largely determined by the security of the critical infrastructure system (Yefimenko et al., 2023; Tzavara & Vassiliadis, 2024). For example, in the European Union, critical infrastructure is defined in accordance with Directive 2008/114/EC, which emphasizes the transnational nature of threats, and NATO pays considerable attention to cyber defense and common approaches to ensuring the resilience of member states (Abgarowicz et al., 2014). Israel has strong cyber defenses and centralized threat management, while Canada focuses on inter-agency coordination and working with private companies. In all countries, an integrated approach that combines legal, organizational, and technological mechanisms is important (Grigalashvili & Abiashvili, 2021). Studying these practices allows us to adapt them to national conditions and form a more effective protection system in Ukraine.

Military security processes are regulated in accordance with the Constitution of Ukraine, the Laws of Ukraine "On National Security of Ukraine," "On the National Security and Defense Council of Ukraine," "On Defense of Ukraine," "On Intelligence," "On the Principles of Domestic and Foreign Policy," "On the Armed Forces of Ukraine," as well as the Decrees of the President of Ukraine "On Issues of the National Security and Defense Council of Ukraine," "On the Decision of the National Security and Defense Council of Ukraine of September 14, 2020, "On the National Security Strategy of Ukraine," "On the Decision of the National Security and Defense Council of Ukraine of March 25, 2021, "On the Military Security Strategy of Ukraine," "On the Decision of the National Security and Defense Council of Ukraine of August 20, 2021 "On the Strategic Defense Bulletin of Ukraine" and Resolutions of the Cabinet of Ministers of Ukraine "On Approval of the Regulations on the Ministry of Defense of Ukraine," "On Approval of the Procedure for Conducting a Defense Review of the Ministry of Defense".

As for Ukraine, the state policy in this area is aimed at predicting threats, preventing crises, reducing risks, and ensuring rapid restoration of facilities in the event of attacks or accidents. Ukraine's regulatory framework defines the legal basis for the protection of critical infrastructure. It includes laws, government regulations and strategic documents in the field of national security. The requirements of international standards and EU directives are partially implemented. There are gaps in the harmonization of legislation with international norms. The need to modernize the legal framework is a key factor in improving the effectiveness of system protection (Herasymenko & Siryi, 2025).

Critical infrastructure is managed by institutions and organizations. Institutions include central bodies and committees. Financial mechanisms include public funding for protection measures and incentives for private investment. Legal mechanisms regulate liability and control over compliance with security standards. The joint application of these mechanisms allows for the integration of resources and optimization of management processes (Demirel et al., 2022).

Risks to critical infrastructure are multifactorial in nature and are classified by source. Natural risks include natural disasters, climate change, and epidemics. Technological risks include accidents at industrial enterprises, transportation, and the energy sector.

Social risks are associated with mass protests, terrorist attacks, and other forms of social destabilization (Ivaniuta et al., 2024). Cyber threats are particularly dangerous because they disrupt digital systems and can paralyze infrastructure networks. Military risks become crucial in the context of hostilities and hybrid aggression. Risk classification allows to systematize threats and develop a comprehensive strategy to prevent them (Table 1).

Table 1. Classification of critical infrastructure risks

Type of risk	Examples of threats	Potential consequences
Natural	Floods, earthquakes, epidemics	Destruction of facilities, disruption of vital services
Technological	Industrial accidents, transportation disasters, power outages	Economic losses, environmental pollution, human casualties
Social	Mass protests, terrorist attacks, social destabilization	Threat to the security of citizens, destabilization of state institutions
Cybernetic	Hacker attacks, cyber espionage, blocking of digital networks	Paralysis of infrastructure systems, data leakage, destabilization of information
Military	Missile and drone attacks, hybrid aggression, sabotage	Destruction of infrastructure, reduction of defense capabilities, large-scale crises

Source: compiled by the author

Table 2. Models of critical infrastructure risk analysis

Model	Characteristics	Advantages	Limitations
Systemic	Considers infrastructure as a single interconnected system	Allows to assess cascading effects	Difficult to apply in practice
Multi-level	Analyzes risks at the facility, regional and national levels	Provides a detailed assessment of threats at different levels	Requires a large amount of data
Cybersecurity	Focuses on information flows and system management	Takes into account digital technologies and cybersecurity	Limited to non-digital threats

Source: compiled by the author

Risk analysis models are an important tool for threat forecasting and defense planning. The cyber model is based on the view of infrastructure as a complex control system where information exchange plays a key role. The system model analyzes the interdependence of all elements and their vulnerability to external influences. The multi-level model involves risk assessment at different levels, from an individual facility to the national system. Such approaches allow identifying both direct and indirect consequences of potential threats (Cherdantseva et al., 2016). The use of models contributes to the development of effective risk management mechanisms and enhanced infrastructure

resilience. The choice of a particular model depends on the specifics of the sector and the nature of potential risks (Table 2).

The development of critical infrastructure crises has different scenarios depending on the scale and nature of the threats. One scenario involves a localized disruption of a single facility with limited impact. Another scenario involves the cascading spread of the crisis to other infrastructure sectors (Heino et al., 2019). A systemic scenario is particularly dangerous when several sectors are disrupted simultaneously. In such circumstances, the state faces the risk of paralyzing key governance and life support functions. The consequences of crisis scenarios include economic losses, social instability, and reduced defense capabilities. The analysis of possible scenarios allows predicting risks and formulating preventive response measures (Krylova & Hlushchenko, 2025).

The digitalization of critical infrastructure increases the efficiency of management and control by providing prompt data collection on the state of systems and possible threats. Monitoring helps to detect and respond to problems in a timely manner, and the use of digital tools increases the resilience of systems and reduces the cascading effects of failures. Thus, digitalization, monitoring, and cybersecurity form the basis of modern critical infrastructure risk management (Lubis et al., 2025).

Modern risk management systems are focused not only on preventing threats, but also on ensuring rapid recovery. The concept of resilience implies the ability of critical infrastructure to withstand and adapt to crisis impacts. It includes preventive measures, monitoring, crisis response, and recovery from incidents. The key principle is an integrated approach that covers organizational, technological and legal levels. The ISO 22301 and NIST standards governing business continuity management are important for implementing this concept. The use of resilience models minimizes cascading effects and increases the reliability of systems (Rehak et al., 2025).

Critical infrastructure protection is impossible without the interaction of the state and business. Most infrastructure facilities are owned by private operators, which increases the importance of partnership models. Public-private partnerships involve joint responsibility for risk management and implementation of security measures. It is important to exchange information between the entities, including data on threats and incidents. Such interaction increases the effectiveness of response and optimizes the use of resources. Examples of partnership initiatives demonstrate the interest of business in ensuring resilience (Ampratwum et al., 2022).

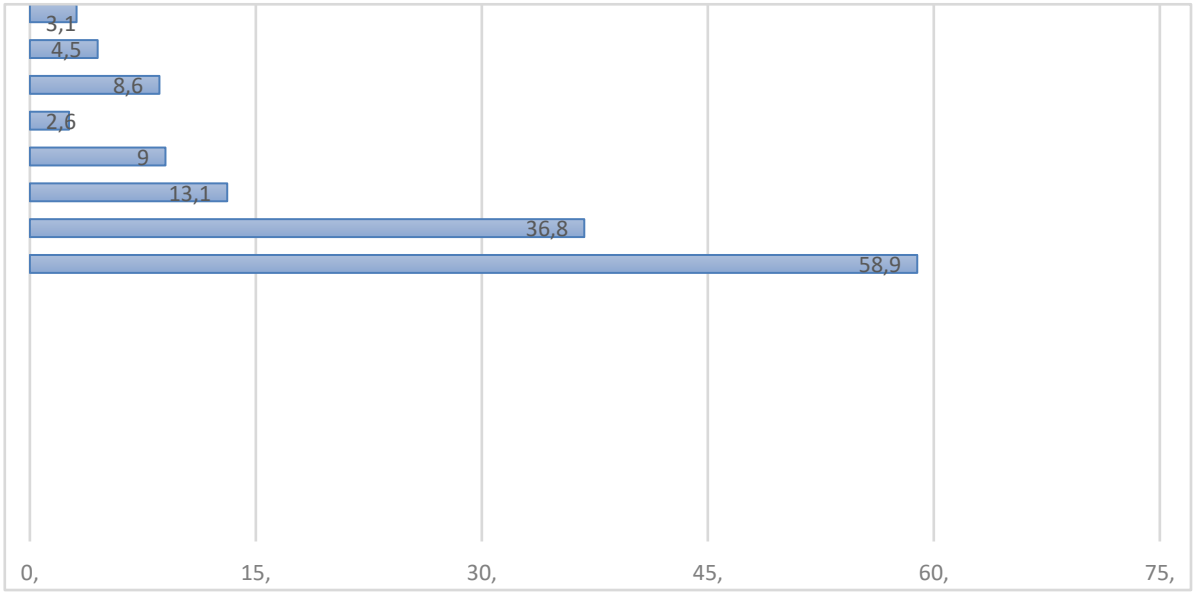
The full-scale war has created unprecedented threats to Ukraine’s critical infrastructure. Massive missile and drone strikes have targeted energy, transportation, and communications. Systematic attacks lead to disruptions in the operation of infrastructure networks and a decrease in the level of life support for the population. The war increases the vulnerability of cyberspace as digital systems become targets of cyberattacks. A particular challenge is the cascading nature of threats, when damage to one sector leads to disruption of other sectors. At the same time, there is a growing need to quickly restore destroyed facilities and ensure their resilience. Thus, the war is shaping a new reality in which the protection of critical infrastructure is a priority for the state (Ivaniuta et al., 2024).

Ukraine declares its desire to harmonize its infrastructure protection system with European and international standards. However, the implementation process faces a number of challenges. The regulatory framework is fragmented and needs to be updated in line with EU and NATO requirements, and government agencies do not have sufficient resources to fully manage risks. Insufficient funding limits infrastructure modernization and cyber defense, making it difficult to implement international approaches.

The main task of creating a comprehensive strategy for the protection of critical infrastructure should be to strengthen coordination between government agencies and the private sector to implement modern resilience standards, create a national cyber defense system, and train specialists (Adegbite et al., 2023).

The energy infrastructure is currently one of the most affected sectors, in particular in terms of the amount of damage caused. In general, the destruction of critical energy, industrial and civilian infrastructure has led to increased security risks, slower investment, and slower socioeconomic development. As of 2024, the amount of direct losses caused by the destruction of infrastructure during the full-scale invasion of Ukraine by Russia between February 2022 and the end of 2023 exceeded 137 billion USD (Figure 3).

Figure 3. Direct losses from the destruction of infrastructure in Ukraine during the full-scale war of the Russian Federation, billion USD February 2022 – end of 2023



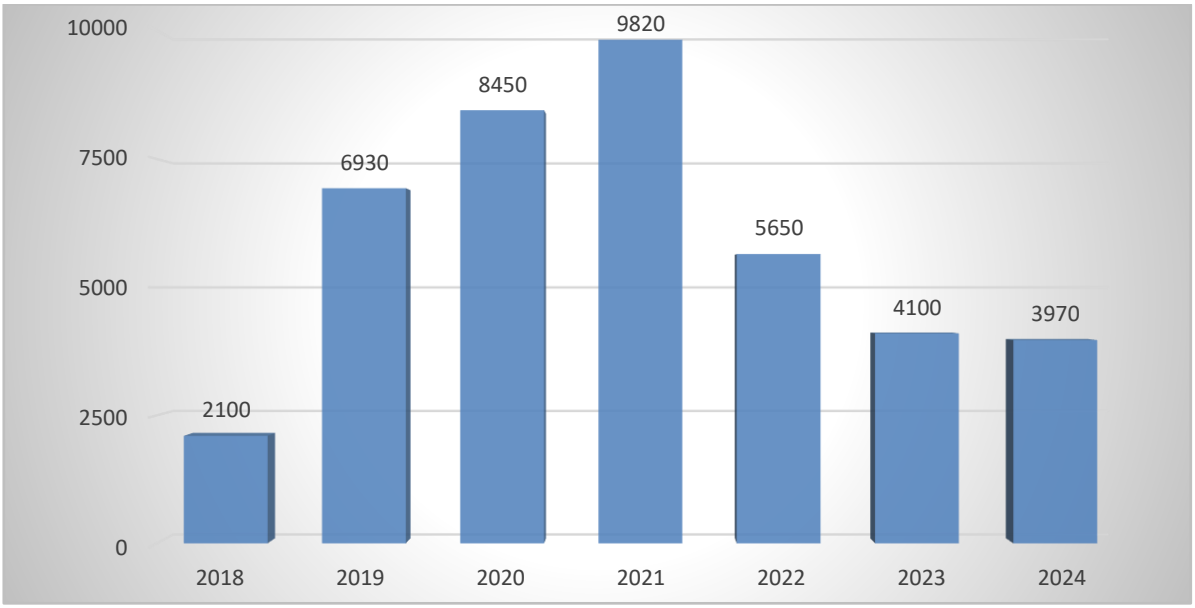
Source: systematized on the basis of the State Statistics Service of Ukraine (2024)

As Figure 3 shows, industrial, energy, and civilian infrastructure suffered the greatest destruction. This situation requires significant financial injections, periodic transfers, and the implementation of a strategy to increase the resilience of energy security.

Ukraine has significant potential in the development of renewable energy, which can strengthen the resilience of energy infrastructure. In order to ensure the fastest possible

balanced development of the industry, Ukraine should deepen the processes of diversification and deregulation, and create conditions for prompt investment. Today, the crisis conditions of the war are causing a slowdown in the industry's development (Figure 4).

Figure 4. Development of renewable energy in Ukraine, MW



Source: compiled by the author based on NKREKP (2024)

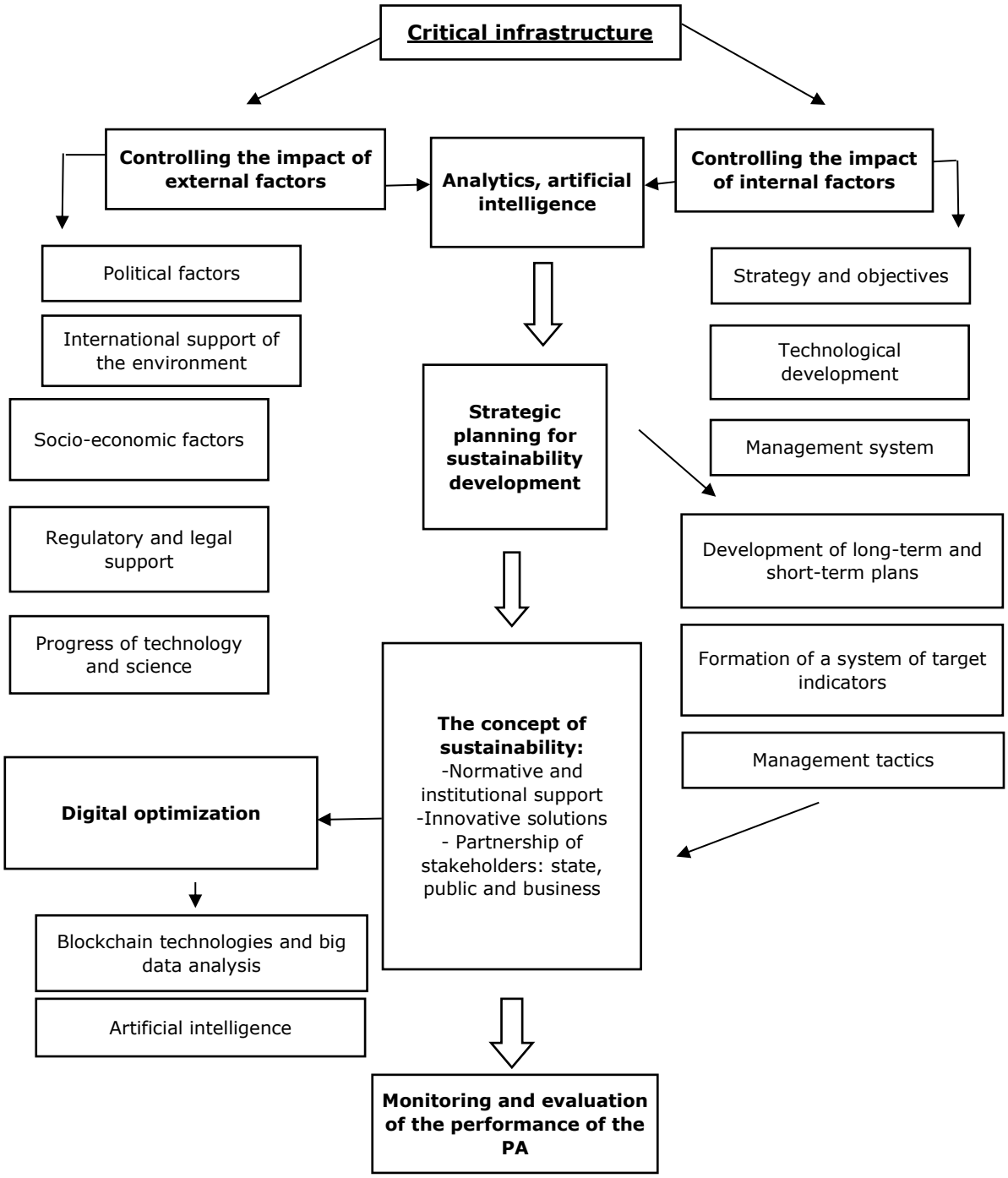
As shown in Figure 4, the full-scale war has made adjustments to the strategy of resource use in the energy sector, as a significant number of alternative energy facilities were destroyed and damaged in the first year of active hostilities.

In order to regenerate critical infrastructure and increase its resilience in wartime crisis conditions, government institutions should implement effective investment development mechanisms, including: war risk insurance for investment projects in priority sectors; interest-free lending for projects to regenerate destroyed or damaged infrastructure; support for industrial and infrastructure investment projects; development of international partnerships; financial incentives for the transfer of green technologies, etc. In particular, the development of a network of industrial parks is positioned as an innovative solution for the rapid restoration of destroyed critical infrastructure, which will contribute to sustainable regional development. This approach will allow for the relocation of production, increase local budgetary injections, and optimize the investment climate. It is also important to further develop the processes of decentralization and deregulation, and to introduce priority models of public-private cooperation.

In addition to the above, it is necessary to use digital technologies and innovative opportunities for data openness, transparency of decision-making procedures for critical infrastructure and control over their implementation, and the implementation of the

necessary corrective action. This approach will ensure high rates of post-war infrastructure regeneration (Figure 5).

Figure 5. Critical Infrastructure Resilience Management Model



Source: Author's elaboration

Analyzing Figure 5, it is necessary to note the importance of integrating digital potential, as electronic information systems allow for the rapid collection and consolidation of necessary data, making informed and reasonable decisions, monitoring and controlling performance. The proposed concept will help to increase the resilience of critical infrastructure, optimize coordination of actions, and strengthen the national security system as a whole.

The events related to the occupation of Crimea and parts of Donetsk and Luhansk regions by the Russian Federation in 2014 prompted the improvement of legal regulation in the field of national critical infrastructure protection in Ukraine. In response to the political situation that developed in late 2014 and early 2015, on January 27, 2016, the President of Ukraine signed a decree enacting the decision of the National Security and Defense Council of Ukraine "On the Cybersecurity Strategy of Ukraine." This document effectively marked the beginning of the formation of legal regulation for the protection of critical infrastructure. The implementation of Ukraine's Cybersecurity Strategy required a number of changes to national legislation to provide a basis for the implementation of its provisions and to increase liability for offences in the field of cybersecurity.

In particular, Resolution No. 563 of the Cabinet of Ministers of Ukraine dated August 23, 2016, approved and enacted the Procedure for forming a list of information and telecommunications systems of critical infrastructure facilities of the state, which for the first time provided an official definition of the concept of "critical infrastructure" as a set of state infrastructure facilities that are most important for the economy and industry, the functioning of society and the safety of the population, and whose failure or destruction could affect national security and defense, the natural environment, and lead to significant financial losses and human casualties.

In order to implement appropriate measures at the national, sectoral, and regional levels regarding legal and organizational-methodological support, coordination, and consolidated provision of resources for security systems, the Cabinet of Ministers of Ukraine, in accordance with the Decision of the National Security and Defense Council of Ukraine dated December 29, 2016 "On improving measures to protect critical infrastructure facilities," developed the Concept for the creation of a state system for the protection of critical infrastructure in Ukraine, which was put into effect by Order of the Cabinet of Ministers of Ukraine No. 1009-r of December 6, 2017.

In particular, the Concept outlines the main problems in the field of building a state system for the protection of critical infrastructure:

- insufficiency and inconsistency of regulatory and legal regulation in Ukraine for the protection of critical infrastructure systems and facilities;

- uncertainty regarding the functions, powers, and responsibilities of central executive bodies and other bodies in the field of critical infrastructure protection, as well as the rights, obligations, and responsibilities of owners and operators of critical infrastructure facilities;

- absence of a state body at the national level responsible for coordinating actions in the field of critical infrastructure protection, existing state protection systems, and crisis response;

- absence of a unified methodology for assessing threats and risks to critical infrastructure, preventing their realization, and responding to threats;

- underdeveloped public-private partnerships and uncertainty regarding sources of funding for critical infrastructure protection measures;

- lack of uniform criteria and methodology for classifying infrastructure facilities as critical infrastructure, and for their certification and categorization;

- insufficient level of international cooperation in this area.

In addition, during this period, important legislative and regulatory acts were adopted, aimed at improving the national security and defense system, in particular, the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" and a number of sector-specific regulatory acts:

- Procedure for forming a list of information and telecommunications systems of critical infrastructure facilities of the state;

- Resolution of the Cabinet of Ministers of Ukraine No. 519 of 19.06.2019 "On Approval of General Requirements for Cyber Protection of Critical Infrastructure Facilities";

- Resolution of the Cabinet of Ministers of Ukraine No. 943 of October 9, 2020, "Certain Issues of Critical Information Infrastructure Facilities";

- Resolution of the Cabinet of Ministers of Ukraine No. 1176 dated November 11, 2020, "On Approval of the Procedure for Reviewing the State of Cyber Protection of Critical Infrastructure, State Information Resources, and Information, the Protection of Which is Required by Law";

- Resolution of the Board of the National Bank of Ukraine No. 151 dated November 30, 2020, "On Approval of the Regulations on the Identification of Critical Infrastructure Objects in the Banking System of Ukraine";

- Resolution of the Cabinet of Ministers of Ukraine No. 1295 dated December 23, 2020, "Certain Issues of Ensuring the Functioning of the System for Identifying Vulnerabilities and Responding to Cyber Incidents and Cyber Attacks";

- Resolution of the Cabinet of Ministers of Ukraine No. 519 dated June 19, 2019, "On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects";

- Resolution of the Cabinet of Ministers of Ukraine No. 1109 dated October 9, 2020, "Certain Issues of Critical Information Infrastructure Facilities";

- Resolution of the Cabinet of Ministers of Ukraine No. 1426 dated December 29, 2021, "On Approval of the Regulations on the Organizational and Technical Model of Cyber Protection."

The concept of "critical infrastructure facility" first appeared in the Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine," but the subject of its regulation is, to a large extent, highly specialized.

With the start of Russia's full-scale invasion of Ukraine, the process of developing a national CII protection system has accelerated significantly. During this period, the main legislative act regulating this activity was enacted – Law of Ukraine No. 1882-IX of November 16, 2021, "On Critical Infrastructure," which came into force only on June 15, 2022. With the adoption of this law, the organizational structure of the CII protection system was outlined at the legislative level; the mechanism for forming the composition of CII was defined by regulation, which created the legal basis for the proper organization of CII and its protection.

The European Union's Global Strategy on Foreign and Security Policy, adopted in 2016, determines the EU's activities in the context of addressing energy security, hybrid transnational threats, migration, and climate change. Among its strategic priorities, the Strategy highlights an integrated approach to crisis management, enhancing the region's defense capabilities, ensuring stability, and developing international cooperation. The Strategy defines the key principles of the EU's positioning in the international arena, namely, upholding the rules of the global order and promoting peace. Ukraine has the potential to be a guarantor of stability in the European region. With active support from the EU and the US, it will be able to realize its own regional ambitions and implement systemic reforms at the state level. At the same time, the process requires adequate security guarantees, which must be formed within the framework of a single effective national security concept.

Discussion

The results show that critical infrastructure is a system of interconnected elements. This is in line with international studies that emphasize the growing role of digital security (Almahmoud et al., 2025). The risk analysis models proposed by the authors demonstrate different levels of effectiveness: the systemic approach allows for the interdependence of sectors, the multi-level model provides details at the facility, regional, and national levels, and the cyber model reveals the role of information flows in system stability. Comparing the findings of scientists with the results of the current study proves the need for a comprehensive combination of approaches.

The effectiveness of practical tools, such as risk and resilience management, is proved by Mitra et al. (2024). In the context of Ukraine, their implementation is hampered by insufficient funding and weak coordination. Public-private partnerships are promising, but need to be strengthened. At the same time, international experience shows that an integration approach provides the highest protection efficiency.

The results of Khrapkina and Metelenko (2025) show the potential for developing the system based on modern risk management models. At the same time, the Ukrainian context requires the adaptation of international standards and the rapid restoration of facilities and their resilience. Obviously, regulatory shortcomings and institutional constraints hinder progress.

In the scientific discourse, the issue of damage to critical infrastructure in wartime has been addressed in publications by Guarini et al. (2021), De Rosa and et al. (2022). In particular, the authors emphasize the scale of Russian attacks on critical infrastructure,

including energy and healthcare systems, and conclude that the main risks point to the need to strengthen resilience for uninterrupted operation. At the same time, Gunawan and Pane (2024) analyze the problem in the context of legal protection, institutional support for assessing damages from the party responsible for the destruction of infrastructure, as well as international guarantees in this regard.

The research of Pacek and Pacek (2023), Gunawan and Pane (2024), Alcaraz and Zeadally (2015) correlates with the results of the current article on the importance of supporting investment regeneration projects and creating security guarantees for critical infrastructure as a basis for socio-economic development.

Thus, the study confirms the strategic role of legal aspects critical infrastructure in the national security system. At the same time, it reveals a gap between international practices and Ukrainian reality. Further research should focus on developing flexible coordination and financing mechanisms.

Conclusions

Critical infrastructure is a key element of national security, ensuring the stability of society and the functioning of state institutions. The analysis of the theoretical and methodological foundations of legal support for the industry has shown that critical infrastructure is a multi-level system with interdependent components. International experience confirms the importance of a comprehensive approach to its protection and implementation of resilience standards.

The study of risks has shown that they are multidimensional and include natural, man-made, social, cyber and military threats. The use of risk analysis models makes it possible to predict consequences and develop preventive measures. Crisis scenarios demonstrate the state's readiness to respond quickly and restore the system's functioning, primarily through effective legal support.

Practical protection tools, such as risk and resilience management systems, increase the efficiency of public administration. Public-private partnerships help coordinate and optimize resources. International best practices show the importance of an integrated approach that includes legal, organizational, and technological mechanisms. The Ukrainian context is characterized by the increased vulnerability of critical infrastructure in times of war. The implementation of international standards is complicated by regulatory, institutional and financial constraints. All of this must be reflected in the national legislative framework and legal support institutions.

Suggestions for improvement include improvement of legal regulationpolicies to strengthen coordination, introduce modern risk management models, develop cyber defense, and improve the legal framework. Implementing these measures will increase the resilience of critical infrastructure, minimize the risks of cascading effects, and ensure national security. An integrated approach based on theoretical models, practical tools, and international experience forms the basis for strategic development and effective management in the industry's legal framework.

References

Abgarowicz, G., Antkiewicz, R., Ciepiela, P., Dyk, M., Dziwisz, D., Fałek, Z., … Wiercińska-Krużewska, A. (2014). *Critical infrastructure security – the ICT dimension.* Kosciuszko Institute. https://www.researchgate.net/publication/283579366_Critical_Infrastructure_Security_-_the_ICT_Dimension

Adegbite, A., Akinwolemiwa, D., Uwaoma, P., Kaggwa, S., Akindote, O., & Dawodu, S. (2023). Review of cybersecurity strategies in protecting national infrastructure: perspectives from the USA. *Computer Science & IT Research Journal, 4*, 200-219. http://doi.org/10.51594/csitrj.v4i3.658

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection, 8*, 53-66. https://doi.org/10.1016/j.ijcip.2014.12.002

Almahmoud, Z., Yoo, P. D., Damiani, E., Choo, K.-K. R., & Yeun, C. Y. (2025). Forecasting Cyber Threats and Pertinent Mitigation Technologies. *Technological Forecasting and Social Change, 210*, 123836. https://doi.org/10.1016/j.techfore.2024.123836

Ampratwum, G., Robert, O.-K., & Tam, P. (2022). Exploring the Concept of Public-Private Partnership in Building Critical Infrastructure Resilience Against Unexpected Events: A systematic Review. *International Journal of Critical Infrastructure Protection, 39*, 100556. https://doi.org/10.1016/j.ijcip.2022.100556

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security, 56*, 1-27. https://doi.org/10.1016/j.cose.2015.09.009

De Rosa, M., Gainsford, K., Pallonetto, F., & Finn, D. P. (2022). Diversification, concentration and renewability of the energy supply in the European Union. *Energy*, *253*. https://doi.org/10.1016/j.energy.2022.124097

Demirel, H. C., Leendertse, W., & Volker, L. (2022). Mechanisms for protecting returns on private investments in public infrastructure projects. *International Journal of Project Management, 40*(3), 155-166. https://doi.org/10.1016/j.ijproman.2021.11.008

Certain issues concerning critical information infrastructure facilities: *Resolution of the Cabinet of Ministers of Ukraine* No. 943 dated October 9, 2020.

Certain issues concerning critical information infrastructure facilities: *Resolution of the Cabinet of Ministers of Ukraine* No. 1109 dated October 9, 2020. Official Gazette of Ukraine. 2020. No. 93 dated November 27, 2020.

Certain issues of ensuring the functioning of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks: *Resolution of the Cabinet of Ministers of Ukraine* No. 1295 dated 23.12.2020. https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text

Dimitropoulos, G. (2020). National security: The role of investment screening mechanisms. In: Chaisse, J., Choukroune, L., Jusoh, S. (Eds.). *Handbook of international*

investment law and policy (pp. 1-37). Springer. https://doi.org/10.1007/978-981-13-5744-2_59-1

Erbas, M., Khalil, S. M., & Tsiopoulos, L. (2024). Systematic literature review of threat modeling and risk assessment in ship cybersecurity. *Ocean Engineering, 306,* 118059. https://doi.org/10.1016/j.oceaneng.2024.118059

Eusgeld, I., Nan, C., & Dietz, S. (2011). "System-of-systems" approach for interdependent critical infrastructures. *Reliability Engineering & System Safety, 96*(6), 679-686. https://doi.org/10.1016/j.ress.2010.12.010

Grigalashvili, V., & Abiashvili, K. (2021, May). Conceptual Review of the European Union Critical Infrastructure Architecture: Policy, Law and Administration. In *Proceedings of the XXIX International Scientific and Practical Conference.* RS Global. http://doi.org/10.31435/rsglobal_conf/25052021/7562

Große, C. (2021). Multi-Level Planning for Enhancing Critical Infrastructure Resilience against Power Shortages – An Analysis of the Swedish System of Styrel. *Infrastructures, 6*(5), 71. https://doi.org/10.3390/infrastructures6050071

Guarini, E., Mori, E., & Zuffada, E. (2021). New development: Embedding the SDGs in city strategic planning and management. *Public Money & Management*, *41*(6), 494-497. https://doi.org/10.1080/09540962.2021.1885820

Gunawan, Y., & Pane, M. (2024). Responsibility for excessive infrastructure damage in attacks: Analysing Russia's Attack in Ukraine. *PETITA: Jurnal Kajian Ilmu Hukum dan Syariah, 9*(1), 212-231. https://doi.org/10.22373/petita.v9i1.213

Heino, O., Takala, A., Jukarainen, P., Kalalahti, J., Kekki, T., & Verho, P. (2019). Critical Infrastructures: The Operational Environment in Cases of Severe Disruption. *Sustainability, 11*(3), 838. https://doi.org/10.3390/su11030838

Herasymenko, O., & Siryi, O. (2025). Regulatory and legal support for international cooperation of the Security service of Ukraine during the fight against criminal offenses at critical infrastructure facilities. *Analytical and Comparative Jurisprudence, 3*, 451-464. http://doi.org/10.24144/2788-6018.2025.03.3.70

Ilyenko, A., Teliushchenko, V., & Dubchak, O. (2025). Modern Cyber Threats To Critical Infrastructure In Ukraine And The World. *Cybersecurity: Education, Science, Technique, 3*, 150-164. http://doi.org/10.28925/2663-4023.2023.27.719

Ingvarson, J., & Hassel, H. (2023). On the strength of arguments related to standardization in risk management regulations. *Safety Science, 158,* 105998. https://doi.org/10.1016/j.ssci.2022.105998

Ivaniuta, S., Panov, E., Ivanenko, O., & Gapon, S. (2024). Assessment of risks to the critical infrastructure of Ukraine in the conditions of russian military aggression. *Proceedings of the NTUU "Igor Sikorsky KPI" Series Chemical engineering ecology and resource saving, 2,* 47-61. http://doi.org/10.20535/2617-9741.2.2024.307360

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management, 8*(2), 100063. https://doi.org/10.1016/j.dim.2023.100063

Kalapodis, N., Sakkas, G., Kazantzidou-Firtinidou, D., Alcasena, F., Cardarilli, M., Eftychidis, G., Schultz, A. (2025). Towards Resilient Critical Infrastructure in the Face of Extreme Wildfire Events: Lessons and Policy Pathways from the US and EU. *Infrastructures, 10*(9), 246. https://doi.org/10.3390/infrastructures10090246

Khrapkina, V., & Metelenko, N. (2025). Adaptation of the world experience in restoring the competitiveness of the real sector of the economy in the regions of Ukraine. *State and Regions*, *1*(135), 20–27. https://www.econom.stateandregions.zp.ua/journal/2025/1_2025/20.pdf

Krylova, I., & Hlushchenko, H. (2025). Evaluation of the effectiveness of current mechanisms for implementing public-private partnerships in Ukraine. *Philosophy and Governance*, *5*(9), art. no. 7. https://doi.org/10.70651/3041-248X/2025.5.07

Li, N., Wang, F., Magoua, J. J., & Fang, D. (2022). Interdependent effects of critical infrastructure systems under different types of disruptions. *International Journal of Disaster Risk Reduction, 81*, 103266. https://doi.org/10.1016/j.ijdrr.2022.103266

Lubis, M., Safitra, M. F., Fakhrurroja, H., & Muttaqin, A. N. (2025). Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience. *Sensors, 25*(15), 4545. https://doi.org/10.3390/s25154545

Mitra, A., Youdon, C., Chauhan, P., & Shaw, R. (2024). Systemic risk capability assessment methodology: A new approach for evaluating inter-connected risks in seaport ecosystems. *Progress in Disaster Science, 22,* 100325. https://doi.org/10.1016/j.pdisas.2024.100325

NKREKP. (2024). National Energy and Utilities Regulatory Commission of Ukraine. https://www.nerc.gov.ua/

Novotny, P., & Janosikova, M. (2020). Designating Regional Elements System in a Critical Infrastructure System in the Context of the Czech Republic. *Systems, 8*(2), 13. https://doi.org/10.3390/systems8020013

Obi, O. C., Odilibe, I. P., & Arowoogun, J. O. (2024). Crisis communication and U.S. national security: A comprehensive review: Understanding the importance of timely and accurate information dissemination. *International Journal of Applied Research in Social Sciences*, *6*(2), 116–139. https://doi.org/10.51594/ijarss.v6i2.779

Pacek, B., & Pacek, P. (2023). Russia's devastating impact on critical infrastructure during the hybrid war in Ukraine. *Security. Theory and Practice, 2*, 11-27. https://www.ceeol.com/search/article-detail?id=1169528

Paravantis, J. A., & Kontoulis, N. (2020). Energy security and renewable energy: a geopolitical perspective. In *Renewable energy-resources, challenges and applications*. IntechOpen. https://doi.org/10.5772/intechopen.91848

Question from the National Security and Defense Council of Ukraine: *Decree of the President of Ukraine* dated February 26, 2021, No. 76/2021. https://zakon.rada.gov.ua/laws/show/76/2021#Text

Procedure for forming a list of information and telecommunications systems of critical infrastructure facilities: *Resolution of the Cabinet of Ministers of Ukraine* No. 563 dated

August 23, 2016. 29. On approval of General requirements for cyber protection of critical infrastructure facilities: *Resolution of the Cabinet of Ministers of Ukraine* dated June 19, 2019, No. 519.

On access to public information. *Law of Ukraine* dated January 13, 2011, No. 2939-VI. https://zakon.rada.gov.ua/laws/show/2939-17

On the principles of domestic and foreign policy: *Law of Ukraine* dated July 1, 2010, No. 2411-VI. https://zakon.rada.gov.ua/laws/show/2411-17#Text

On the protection of personal data. *Law of Ukraine* dated 01.06.2010 No. 2297-VI. https://zakon.rada.gov.ua/laws/show/2297-17

On approval of the procedure for reviewing the state of cyber protection of critical infrastructure, state information resources, and information, the protection requirements for which are established by law: *Resolution of the Cabinet of Ministers of Ukraine* No. 1176 dated November 11, 2020.

On approval of the procedure for reviewing the state of cyber protection of critical infrastructure, state information resources and information, the protection requirements for which are established by law: *Resolution of the Cabinet of Ministers of Ukraine* No. 1176 dated 11 November 2020.

On approval of the Regulations on the identification of critical infrastructure objects in the banking system of Ukraine: *Resolution of the Board of the NBU* No. 151 dated November 30, 2020.

On approval of the Regulations on the organizational and technical model of cyber protection: *Resolution of the Cabinet of Ministers of Ukraine* No. 1426 dated December 29, 2021.

On Information. *Law of Ukraine* No. 2657-XII dated October 2, 1992. https://zakon.rada.gov.ua/laws/show/2657-12

On media. *Law of Ukraine* No. 2710-IX of December 13, 2022. –. https://zakon.rada.gov.ua/laws/show/2710-20

On the basic principles of ensuring cybersecurity in Ukraine: Law of Ukraine No. 2163-VIII of October 5, 2017.

On the basic principles of ensuring cybersecurity in Ukraine: Law of Ukraine No. 2163-VIII of October 5, 2017.

On critical infrastructure: Law of Ukraine No. 1882-IX of November 16, 2021.

On the defense of Ukraine: Law of Ukraine No. 1932-XII of December 6, 1991. No. 1932-XII. https://zakon.rada.gov.ua/laws/main/1932-12#Text

On the Fundamentals of National Resistance: Law of Ukraine dated 16.07.2021 No. 1702-IX. https://zakon.rada.gov.ua/laws/show/1702-20#Text

On the Legal Regime of a State of Emergency Law of Ukraine dated March 16, 2000, No. 1550-III.

On the National Security and Defense Council of Ukraine: Law of Ukraine No. 183/98-VR dated March 5, 1998. https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text

On the Cybersecurity Strategy of Ukraine: Decree of the President of Ukraine No. 96/2016 of March 15, 2016, "On the Decision of the National Security and Defense Council of Ukraine of January 27, 2016.

On improving measures to protect critical infrastructure: *Decree of the President of Ukraine* No. 32/2017 of February 13, 2017, "On the decision of the National Security and Defense Council of Ukraine of December 29, 2016, "On threats to the cybersecurity of the state and urgent measures to neutralize them."

Rass, S., Schauer, S., König, S., & Zhu, Q. (2020). *Cyber-Security in Critical Infrastructures*. Springer International Publishing. https://doi.org/10.1007/978-3-030-46908-5

Rehak, D., Splichalova, A., Janeckova, H., Ryska, O., Oulehlova, A., Michalcova, L., & Ristvej, J. (2025). Critical entities resilience strengthening tools to small-scale disasters. *International Journal of Critical Infrastructure Protection, 49*, 100766. https://doi.org/10.1016/j.ijcip.2025.100766

Roshanaei, M. (2021). Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. *Journal of Computer and Communications, 9*, 80-102. http:/doi.org/10.4236/jcc.2021.98006

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors, 23*(15), 6666. https://doi.org/10.3390/s23156666

State Statistics Service of Ukraine. (2024). https://www.ukrstat.gov.ua

Strategic Defense Bulletin of Ukraine: Decree of the President of Ukraine "On the Decision of the National Security and Defense Council of Ukraine of August 20, 2021 "On the Strategic Defense Bulletin of Ukraine" dated September 17, 2021 No. 473/2021. https://zakon.rada.gov.ua/laws/show/ 473/2021#n2

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: a historical and conceptual review. *International Journal of Information Security, 23*(3), 1695-1719. https://doi.org/10.1007/s10207-023-00811-x

UKRAINE Third Rapid Damage and Needs Assessment (RDNA3) February 2022 – December 2023. (2024). *World Bank Group*. https://ukraine.un.org/sites/default/files/2024-02/UA%20RDNA3%20report%20EN.pdf

Yefimenko, I., Sakovskyi, A., & Bilozorov, Y. (2023). Protection of critical infrastructure as a component of Ukraine's national security. *Law Journal of the National Academy of Internal Affairs*, *13*(2), 74–85. https://doi.org/10.56215/naia-chasopis/2.2023.74