DOI: 10.31617/1.2025(159)03
UDC 339.92:[061.1ЄС:1-622(477)=111

SHKUROPADSKA Diana,
PhD (Economics),
Associate Professor of the Department
of Economics and Competition Policy
State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine

ORCID: 0000-0002-6883-711X
diana.shkuropadska2016@knute.edu.ua

LEBEDEVA Larysa,
PhD (Economics),
Associate Professor,
Associate Professor of the Department
of Economics and Competition Policy
State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine

ORCID: 0000-0001-8632-5460
l.lebedeva@knute.edu.ua

GONÇALVES Jorge,
PhD (Geography), Associate Professor,
Institut Superior Tecnico – University
of Lisbon,
Avenida Rovisco Pais, 1, 1049-001, Lisboa, Portugal

ORCID: 0000-0001-6781-5149
jorgemgoncalves@tecnico.ulisboa.pt

INSTITUTIONAL FRAMEWORK FOR THE RESILIENCE OF CRITICAL INFRASTRUCTURE OF EU, NATO COUNTRIES AND UKRAINE

The necessity of protecting critical infrastructure is an extremely important task for the normal functioning of the national states, especially taking into account modern threats related to military actions, natural disasters, cyberattacks, pandemics, etc. The aim of the research is to substantiate and characterize the organizational and legal conditions for ensuring the resilience of critical infrastructure, using the example of the EU, NATO countries and Ukraine. The article's hypothesis is that the resilience of critical infrastructure depends on the level of institutional support, which is capable of adapting to the conditions of modern threats and risks, particularly during wartime, and involves comprehensive interaction between state institutions, the private and international organizations. To achieve the aim of the research, a

ШКУРОПАДСЬКА Діана,
доктор філософії, доцент кафедри економічної
теорії та конкурентної політики
Державного торговельно-економічного
університету
вул. Кіото, 19, м. Київ, 02156, Україна

ORCID: 0000-0002-6883-711X
diana.shkuropadska2016@knute.edu.ua

ЛЕБЕДЕВА Лариса,
к. е. н., доцент, доцент кафедри економічної
теорії та конкурентної політики
Державного торговельно-економічного
університету
вул. Кіото, 19, м. Київ, 02156, Україна

ORCID: 0000-0001-8632-5460
l.lebedeva@knute.edu.ua

ГОНСАЛВЕС Жорже,
к. геогр.н., доцент,
Вищий технічний інститут –
Лісабонський університет
Авеніда Ровішку Пайш, 1, 1049-001, Лісабон,
Португалія

ORCID: 0000-0001-6781-5149
jorgemgoncalves@tecnico.ulisboa.pt

ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЄС, НАТО ТА УКРАЇНИ

Захист критичної інфраструктури є надзвичайно важливим завданням для забезпечення стабільного функціонування держави, особливо в умовах сучасних загроз, пов'язаних з військовими конфліктами, природними катастрофами, кібератаками, пандеміями тощо. Метою дослідження є обґрунтування організаційно-правових умов забезпечення стійкості критичної інфраструктури на прикладі країн ЄС, НАТО та України. У ході дослідження перевірено гіпотезу, що стійкість критичної інфраструктури залежить від рівня інституційного забезпечення, яке здатне адаптуватися до умов сучасних загроз і ризиків, зокрема у воєнний час, і включає комплексну взаємодію між державними інститутами, приватним сектором та міжнародними організаціями.

complex of general scientific and special methods was used, including methods of systematization and generalization, tabular methods, as well as analysis and synthesis.

The main regulatory legal acts ensuring the resilience of critical infrastructure in the EU have been identified and analyzed, highlighting the importance of coordinated efforts among EU member states to enhance the resilience and protection of critical infrastructure, especially in response to cross-border threats. NATO approach to ensuring the resilience of critical infrastructure has been analyzed that focuses primarily on crisis preparedness and ensuring the continuity of governance and essential functions even in the event of military aggression or hybrid threats. The regulatory legal acts on ensuring the resilience of critical infrastructure in Ukraine have also been examined, and the main tasks of the authorities responsible for ensuring the resilience of critical infrastructure identified. The levels and management bodies of Ukraine's national system for protecting critical infrastructure have been defined.

The main determinants of the resilience of critical infrastructure entities include physical resilience, functional resilience, organizational resilience, informational resilience, social resilience, economic resilience, and environmental resilience. These determinants are interconnected and collectively impact the ability of critical infrastructure entities to ensure continuous operation in crisis situations.

Keywords: critical infrastructure, resilience, institutional conditions, risks, crisis situation.

Для досягнення мети використано комплекс загальнонаукових та спеціальних методів: систематизації та узагальнення; табличний; аналізу та синтезу. Розглянуто основні нормативно-правові акти забезпечення стійкості критичної інфраструктури ЄС, що підкреслюють важливість скоординованих зусиль між державами – членами ЄС для підвищення стійкості та захисту критичної інфраструктури, особливо у відповідь на транскордонні загрози. Проаналізовано підхід НАТО до забезпечення стійкості критичної інфраструктури. Акцентовано на готовності до кризових ситуацій і забезпеченні безперервності управління та основних функцій навіть у разі воєнної агресії або гібридних загроз. Проаналізовані нормативно-правові акти щодо забезпечення стійкості критичної інфраструктури України, визначені основні завдання органів забезпечення стійкості критичної інфраструктури. Зазначені рівні та органи управління національною системою захисту критичної інфраструктури України. Основними детермінантами стійкості об'єктів критичної інфраструктури є: фізична, функціональна, організаційна, інформаційна, соціальна, економічна та екологічна стійкість. Ці детермінанти взаємопов'язані та комплексно формують здатність об'єктів критичної інфраструктури забезпечувати безперервне функціонування у кризових ситуаціях.

Ключові слова: критична інфраструктура, стійкість, інституційні умови, ризики, кризова ситуація.

JEL Classification: H12, H54, F53, L78, O43, O52.

Introduction

Critical infrastructure is a set of facilities that are extremely important for the functioning of society and the country's economy. This infrastructure primarily includes defence facilities, as well as those that provide essential services and communication. It may consist of power plants, water supply systems, food production and storage facilities, key transportation hubs, telecommunication networks, medical institutions, and many other priority objects. Ensuring the safety and functioning of these facilities under normal conditions, as well as during emergencies such as martial law, is one of the state's priorities.

The need to protect critical infrastructure is an extremely important task for the normal functioning of the state, especially during modern threats related to military actions, natural disasters, cyberattacks, pandemics etc. In this regard, governments in many countries are strengthening resilience measures (Mukherjee et al., 2023) for facilities considered critical to the livelihood of society.

Ukrainian and foreign researchers are actively studying the problem of critical infrastructure resilience of countries. Scientists emphasize that, within the paradigm of critical infrastructure protection, stakeholders have traditionally approached risk management with an asset-based focus, prioritizing security and physical measures to fully prevent disruptions to critical infrastructure (OECD, 2019, April 17, Ch. 2).

The key priorities for enhancing critical infrastructure resilience include: comprehensive enhancement of the legal framework for its protection; establishment of a state management system for its security; strengthening the safeguarding of critical infrastructure, particularly within the energy and transport sectors; fostering collaboration among entities involved in critical infrastructure protection; and promoting public-private partnerships in emergency prevention and response (Melnychuk, 2021; Yang et al., 2023).

Modern policies for critical infrastructure resilience must consider diverse and complex shock events, more interdependent systems and countries, and the rapid pace of innovation in infrastructure sectors (Khrapkina, 2024). It is also emphasized that protecting critical infrastructure requires partnership interaction between the owners and operators of critical infrastructure on one side and government agencies on the other (NISS, 2013, December 9). The public and private sectors hold a shared responsibility for critical infrastructure resilience, requiring the formation of a robust partnership and a high level of trust to facilitate the effective exchange of sensitive information (Ninković, 2021). Moreover, economists state that institutional conditions for ensuring economic resilience can reduce the vulnerability of the economic system to shocks, promote effective countermeasures, and accelerate economic recovery after such events. The development of institutional conditions depends on effective public policy and mechanisms for counteracting shocks (Lagutin et al., 2020).

Researchers emphasize that today's critical infrastructure is largely digital, with cyber-physical systems playing a central role. These systems integrate computing technologies with physical processes, resulting in digital-physical hybrids that are foundational to our infrastructure. This cyber-physical nature now characterizes sectors such as water, electricity, communications, healthcare, transportation, manufacturing, and defense (Horvitz, 2024).

Key indicators commonly used to measure critical infrastructure resilience include: organizational resilience; performance degradation, disruption, and recovery processes; resilience metrics and indices; safety, security, and risk assessments; societal/community resilience and social equity considerations; dynamic network connectivity; resilience through design and structural robustness; and economic resilience (Osei-Kyei et al., 2022).

It is also noted that national resilience largely depends on the resilience of economic sectors, as the country's economic system is the foundation for its security, well-being, and development. The resilience of economic sectors affects the country's ability to withstand external and internal threats, as well as to recover quickly from crises (Umantsiv & Shkuropadska, 2023).

Ukraine, under martial law, has demonstrated the vulnerability of its energy, transport, and information infrastructure to targeted destruction. EU and NATO countries have significant experience and mechanisms to ensure the resilience of critical infrastructure, while in Ukraine, these systems need strengthening in the face of Russian aggression. Ukraine's integration into European and Euro-Atlantic structures requires harmonizing approaches to critical infrastructure protection. After the war, the restoration of Ukraine's critical infrastructure will require modern approaches that incorporate the experiences of the EU and NATO.

The aim of the research is to substantiate and characterize the organizational and legal conditions for ensuring the resilience of critical infrastructure, using the example of the EU, NATO countries and Ukraine.

The article's hypothesis is that the resilience of critical infrastructure depends on the level of institutional support, which can adapt to the conditions of modern threats and risks, particularly during wartime, and involves comprehensive interaction between state institutions, the private sector, and international organizations. The hypothesis suggests that the foundation for ensuring resilience lies in the institutional component, which can either strengthen or weaken the level of protection of critical infrastructure.

To achieve the aim of the research, a combination of general scientific and specific methods was used: methods of systematization and generalization to identify the organizational and legal conditions for ensuring the resilience of critical infrastructure in EU and NATO countries; a tabular method for analysing the organizational and legal conditions for ensuring the resilience of Ukraine's critical infrastructure; analysis and synthesis for identifying the factors that ensure the resilience of critical infrastructure objects.

The structure of the article is as follows: first, the organizational and legal conditions for ensuring the resilience of critical infrastructure in EU and NATO countries are analysed; next, the organizational and legal conditions for ensuring the resilience of Ukraine's critical infrastructure are examined; finally, the determinants for ensuring the resilience of critical infrastructure objects are highlighted; and conclusions.

1. Organizational and legal conditions for ensuring resilience of the EU critical infrastructure

Considering the probability of new challenges and threats to life safety, particularly those resulting from Russia's aggression against Ukraine, the European Union recognized the need to coordinate the actions of member states, national authorities, EU institutions, and critical infrastructure operators to ensure the resilience of essential services in the EU market. In December 2022, the EU Council adopted the "Recommendations for a Coordinated Approach to the Resilience of Critical Infrastructure". It specifically recommended introducing the necessary tools and coordinating actions at the EU level to improve preparedness and response to security incidents threatening the provision of essential services within the EU internal market.

The EU Council also adopted the "Directive on the Resilience of Critical Entities" (which took effect on January 16, 2023). The Critical Entities Resilience (CER) Directive establishes a framework to support member states in ensuring that critical entities can prevent, withstand, absorb, and recover from disruptive incidents, including those caused by natural disasters, terrorism, internal threats, sabotage, civil unrest, or public health emergencies. The regulatory framework for the EU's critical infrastructure resilience policy is presented in *Table 1*.

Table 1

The regulatory framework for the EU critical infrastructure resilience policy

Name of the document	Number, date of acceptance	Purpose
Directive on the resilience of critical entities (CER Directive)	2022/2557, 14 December 2022	The directive provides for strengthening coordination, risk assessment, ensuring continuity of operation and establishing a monitoring and reporting system to improve safety and resilience of critical facilities
Impact Assessment of the proposed CER Directive	SWD/2020/358 final, 16 December 2020	To analyze the potential consequences and effectiveness of the proposed measures to increase the resilience of critical infrastructure. The document provides a rationale for proposed policies, assessing their impact on safety, economy, social aspects and the environment, helping to make informed decisions about the implementation of new regulations
Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure	2023/C 20/01, 8 December 2022	To ensure joint action and coordination between EU member states to increase protection and resilience of critical facilities. These recommendations aim to facilitate the exchange of information, best practices and resources to effectively respond to threats and incidents that may affect the security and operation of critical infrastructure in the EU
Council Recommendation on a blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance	C/2024/4371, 25 June 2024	To ensure a coordinated and effective response to disruptions that have a cross-border impact. The recommendations are aimed at strengthening cooperation between member states, ensuring rapid information exchange, mobilizing resources and coordinating actions to minimize the negative consequences of such disruptions for the security, economy and well-being of EU citizens
Commission Staff Working Document: Evaluation of ECI Directive	SWD (2019) 308 final, 23 July 2019	To assess the effectiveness of the implementation of the European Critical Infrastructure Directive (ECI Directive). This document analyzes the extent to which the directive's objectives have been achieved, identifies the strengths and weaknesses of its implementation, and provides recommendations for possible improvements to enhance the level of protection of critical infrastructure in the EU
European Critical Infrastructure (ECI) Directive	2008/114/EC, 8 December 2008	To increase the level of protection of critical infrastructure in the European Union. This directive establishes processes and measures for the identification and protection of critical objects that are important for maintaining the life of society, the economy and security, in particular in the event of terrorist attacks or other threats

Source: compiled by the authors based on data from (European Commission, 2024, September 23).

At the beginning of 2023, the synchronization of efforts between the EU and NATO to ensure the resilience of critical infrastructure was announced. The goal of strengthening the EU critical infrastructure resilience policy is to enhance the capacity of member states to improve resilience in the provision of services that are essential for maintaining vital societal functions, economic activities, public health, safety, and the environment in the EU. The CER Directive covers eleven sectors of critical infrastructure (*Figure 1*).

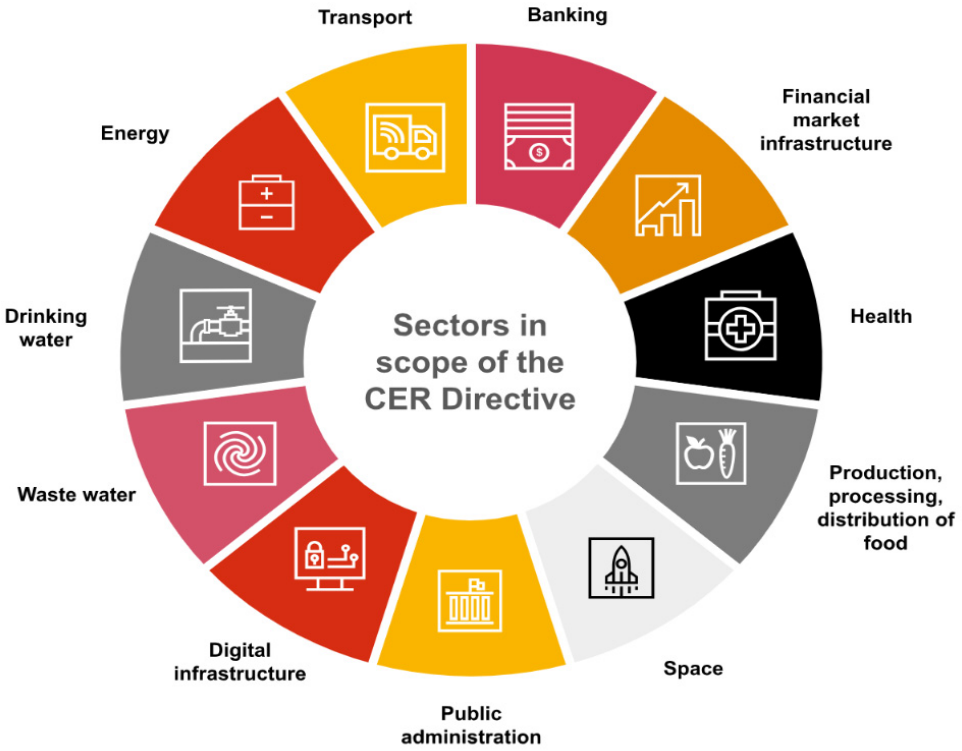

Figure 1. Sectors of critical infrastructure in the EU

Source: compiled by the authors based on data from (PwC, n. d.).

The aim of The Critical Infrastructure Resilience Group (CIRG) is to facilitate cooperation between Member States and with the European Commission, in order exchange experience from implementing best practices on improving the characteristics of critical infrastructure resilience.

Our sectoral analysis of critical infrastructure resilience in transport logistics, energy, healthcare, and food in the EU and Ukraine highlights the following resilience factors:

In transport Logistics: efficiency in customs and border procedures, quality of trade and transport infrastructure, cost-effective international shipping, quality of logistics services, and reliable tracking and timely delivery (Lebedeva & Shkuropadska, 2024a).

In energy: geopolitical stability, energy resource availability, robust infrastructure, risk management, energy-efficient technologies, and transparent regulations (Lebedeva & Shkuropadska, 2024b).

In healthcare: preparedness, resource allocation, data analytics, communication, public trust, and adaptive policies–key factors during the pandemic (Lebedeva & Shkuropadska, 2024c).

In Food: diversifying agricultural production through increased capitalization and investment in agro-enterprises, enhancing resource efficiency, food resilience, market institutions, and higher value-added exports (Shkuropadska et al., 2024).

2. Organizational and legal conditions for ensuring resilience of NATO critical infrastructure

Since the early 1950s, NATO has taken efforts in fostering and enhancing civil preparedness among its member states. The concept of resilience is described in Article 3 of the Alliance's Founding Treaty, which obligates member states to "maintain and develop their individual and collective capacity to resist armed attack". This commitment includes ensuring the continuity of government operations, maintaining essential services, and providing civil support for military efforts within member nations (Roepke & Thankey, 2019).

NATO identifies such sectors of critical infrastructure to ensure national and international security (*Figure 2*).

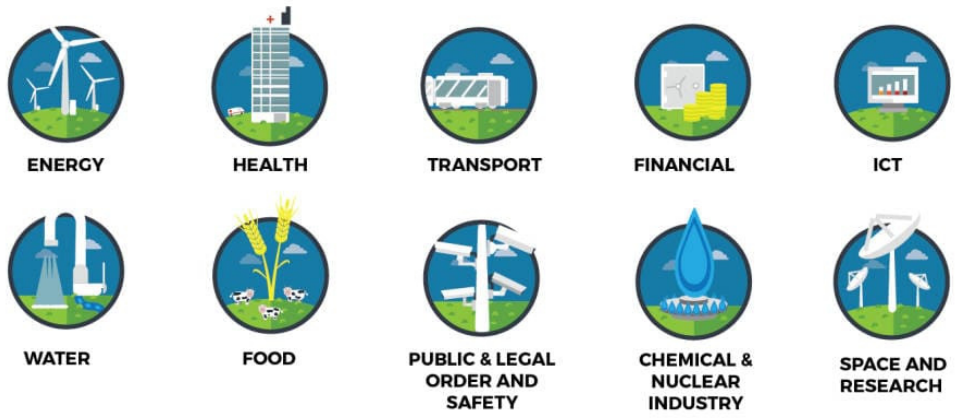

Figure 2. Sectors of Critical Infrastructure in NATO countries

Source: Roepke & Thankey, 2019, February 27.

During the Cold War, NATO civil preparedness was highly organized. However, the 1990s saw significant reductions in plans, structures, and resources at both national and NATO levels. Events after 2014, including Russia's annexation of Crimea and the rise of ISIS/Daesh, highlighted a shifting strategic environment, prompting NATO to enhance its defense. Simultaneously, growing terrorist and hybrid threats, such as cyberattacks on critical infrastructure, highlited the need to strengthen civil preparedness as a cornerstone of resilience (Becker et al., 2022).

At the 2016 Warsaw Summit, NATO leaders committed to seven core civil preparedness requirements (NATO Summit Guide, 2016, July):

- Maintaining governance and essential public services;
- Ensuring resilient energy supplies;
- Managing large population movements;
- Securing food and water supplies;
- Addressing mass casualties;
- Protecting civil communication systems;
- Safeguarding public transportation.

In 2021, NATO emphasized that resilience is essential for credible defense and the protection of society and shared values. Recent years have shown that military efforts alone cannot ensure security, highlighting the need for effective civil defense system to reduce risks during both war and peace.

Military forces increasingly depend on civilian resources for transport, communications, and supplies like water and food. Post-Cold War defense budget cuts have deepened this reliance, with much critical infrastructure privately owned. For example, 90% of military transport for large operations comes from commercial entities, 30% of defense satellite communications are provided by private companies, and local commercial infrastructure supplies 75% of NATO operational support (Shelest, 2021).

Ukraine's cooperation with NATO during the full-scale war has become a crucial element in strengthening Ukraine's defence capabilities and ensuring its ability to counter russia's aggression. The Alliance also emphasizes the importance of supporting Ukraine on its path to future NATO membership, which is a significant step toward ensuring resilience and security in Europe.

3. Organizational and legal conditions for ensuring the resilience of Ukrainian critical infrastructure

Ukrainian legislation on critical infrastructure and its protection comprises the Constitution of Ukraine, the Law "On Critical Infrastructure", the Cabinet of Ministers' decree "On the Approval of the National Plan for the Protection, Security, and Resilience of Critical Infrastructure", international treaties ratified by the Verkhovna Rada of Ukraine, and other relevant legal acts. The protection and legal regime of critical infrastructure objects during emergencies, martial law, or special periods are regulated by the Law "On the Legal Regime of Martial Law", the Law "On the Legal Regime of Emergency Situations", the Law "On the Functioning of Ukraine's Unified Transport System in a Special Period", and the Law "On the Defence of Ukraine".

The Law "On Critical Infrastructure" (dated November 16, 2021, No. 1882-IX) defines resilience as the ability of critical infrastructure to

function normally, adapt to changing conditions, and recover quickly from threats. It outlines tasks such as preventing unauthorized interference, establishing a national protection system, creating regulatory frameworks, and developing state programs to enhance infrastructure security and resilience, as well as ensuring international cooperation in the field.

The national system for the protection of critical infrastructure includes various management levels: national, regional and sectoral, local, and facility-specific (*Table 2*).

Table 2

Levels of management of the national system for protection of critical infrastructure of Ukraine

Management levels	Responsible entities
National level	Management is carried out by the Cabinet of Ministers of Ukraine, the authorized body for critical infrastructure protection in Ukraine, government authorities according to their jurisdiction, other central executive bodies and state agencies, as well as the National Bank of Ukraine
Regional and sectoral levels	Management carried out by central and local executive authorities, designated in accordance with the established legal procedure as responsible for ensuring the formation and implementation of state policy in the area of critical infrastructure protection in a specific sector of critical infrastructure, and responsible for the functioning of individual state protection and response systems
Local level	Management carried out by local executive authorities (military-civil administrations, if established) and local self-government bodies
Facility level	Management carried out by the critical infrastructure operator based on regulatory and legal acts in the area of critical infrastructure protection

Source: compiled by the authors based on data from (Law of Ukraine "On Critical Infrastructure", 2024, September 21).

To organize the functioning of the national critical infrastructure protection system, the Cabinet of Ministers of Ukraine, central executive authorities, local executive authorities (military-civil administrations, if established), and local self-government bodies develop and approve relevant crisis response plans and programs.

The features of implementing state policy in the area of critical infrastructure protection are identified for critical infrastructure sectors. The formation and implementation of state policy in the relevant sectors are carried out by sectoral bodies within critical infrastructure protection. Sectoral bodies in this field maintain sectoral lists of critical infrastructure facilities. The list of critical infrastructure sectors and entities responsible for forming and implementing state policy in the respective sectors of the national critical infrastructure protection system are defined by the Cabinet of Ministers of Ukraine. The Law of Ukraine "On Critical Infrastructure" (2024, September 21) includes the following in the list of vital functions and/or services, the violation of which leads to negative consequences for the

national security of Ukraine: management and provision of the most important public (administrative) services; energy supply (including thermal energy supply); water supply and drainage; food security; health care; pharmaceutical industry; production of vaccines, sustainable functioning of biolaboratories; information services; electronic communications; financial services; transportation support; defence, state security; law and order, administration of justice, detention; civil protection of the population and territories, rescue services; space activities, space technologies and services; chemical industry; research activity.

To determine the level of requirements for ensuring the protection of critical infrastructure facilities according to their importance for providing specific vital functions within the sectors of critical infrastructure, a categorization of critical infrastructure facilities is conducted based on criticality categories:

I Critical Category – particularly important facilities that have national significance, a substantial impact on other critical infrastructure facilities, and whose disruption would lead to a crisis situation of national significance;

II Critical Category – vital facilities, the disruption of which would lead to a crisis situation of regional significance;

III Critical Category – important facilities, the disruption of which would lead to a crisis situation of local significance;

IV Critical Category – necessary facilities, the disruption of which would lead to a crisis situation of local significance.

The categorization of critical infrastructure facilities is carried out by sectoral bodies in the area of critical infrastructure protection according to sectoral specifics and the requirements of sectoral legislation. Sectoral bodies, together with critical infrastructure operators, carry out the categorization of critical infrastructure facilities within their sectors (subsectors) in accordance with the Methodology for Categorizing Critical Infrastructure Facilities.

Entities within the national critical infrastructure protection system develop a cooperation plan with each other, which is coordinated with the authorized body for critical infrastructure protection in Ukraine and approved by the Cabinet of Ministers of Ukraine, and reviewed every three years. The cooperation plan may define the specifics of interaction for the operational modes of the national critical infrastructure protection system.

4. Determinants of ensuring the resilience of critical infrastructure facilities

The full-scale invasion of Russia has caused significant damage to Ukrainian critical infrastructure, leading to substantial disruptions in the provision of essential utility services. Subsequent targeted attacks have

severely impacted drainage, water, heating, and electricity supply systems, and have also resulted in the destruction of residential buildings, schools, and medical facilities. Given such extensive consequences, the repair and reconstruction of critical infrastructure have become urgent priorities.

To address these pressing needs, in December 2022, the European Union and NEFCO launched a EUR 50 million initiative for the restoration of key municipal infrastructure in 12 communities in Kyiv Oblast. These projects fall under Component I of the program. Despite the war, and partly due to it, the initiative has made significant progress as over 80% of planned procurements have been initiated. In 2024, the program was expanded to include five additional projects to modernize critical utility services such as water supply, drainage, and heating in Chernihiv, Sumy, and Mykolaiv Regions. The program is expected to benefit 245 000 residents, reducing electricity consumption by approximately 17 000 MWh per year and cutting greenhouse gas emissions by 15 700 tons of CO_2 annually (EEAS. Delegation of the European Union to Ukraine, 2024, May 22).

It is important to note that critical infrastructure facilities, such as power plants, transport hubs, telecommunications networks, and other enterprises, are among the highest priorities. They have a higher level of protection and are provided with energy and other resources as a priority. For the protection of Ukraine's critical information infrastructure, which is fundamental to the country's stable functioning, it is essential to ensure not only physical protection but also cybersecurity measures for critical infrastructure facilities. Cyberattacks have occurred repeatedly, so all facilities connected to the internet require reliable cybersecurity measures.

Today, the registry includes many facilities of varying degrees of importance, such as ports and industrial enterprises that produce armaments for the front and maintain Ukraine's defence. Essentially, while the country's economy is on a military footing, it also affects the situation in this area. The registry may also include vital bridges upon which the functioning of the state's arteries and the supply of weapons to the front depend.

To protect these facilities, the Ukrainian government has approved a critical infrastructure protection policy for 2024. According to this policy, important infrastructure facilities must be protected from potential threats and attacks by hostile forces. In particular, the placement of air defence systems in the country is carried out taking into account the criticality of the facilities that need protection from enemy attacks and technogenic disasters (Kyiv Post, 2024, February 19).

Thus, the determinants of critical infrastructure resilience are a combination of factors that influence the ability of infrastructure facilities to withstand and recover from various types of impacts (*Table 3*).

Table 3

Determinants of the resilience of critical infrastructure facilities

Factors	Essence
Physical resilience	The strength and reliability of buildings, structures and technical systems, the ability to withstand shocks
Functional resilience	The ability of infrastructure objects to maintain or quickly restore functionality after an interruption or damage
Organizational resilience	Effectiveness of management and coordination of actions in emergency situations, readiness of personnel to act in emergency conditions
Informational resilience	The ability to protect and restore information systems and data important for the functioning of the infrastructure
Social resilience	The ability of society to support the functioning of critical infrastructure objects, the interaction of citizens and their trust in the actions of authorities in crisis situations
Economic resilience	Financial capacity to ensure restoration and modernization of critical infrastructure facilities, availability of resources for rapid response to crises
Environmental resilience	The ability of critical infrastructure facilities to minimize the negative impact on the environment and adapt to climate change and other environmental challenges

Source: compiled by the authors.

The main determinants of the resilience of critical infrastructure entities include: physical resilience, functional resilience, organizational resilience, informational resilience, social resilience, economic resilience, and environmental resilience. These determinants are interconnected and collectively impact the ability of critical infrastructure entities to ensure continuous operation in crisis situations. Let's consider specific examples that demonstrate the interrelationship between various determinants of critical infrastructure resilience:

Physical and Functional Resilience. Recovery from floods in Germany in 2021. Infrastructure such as bridges and roads was physically damaged, leading to disruptions in transportation routes and the supply of goods. It was necessary not only to repair these facilities but also to ensure they quickly regained functionality, which required a comprehensive approach to repair and recovery management (Witting, 2023).

Organizational and Informational Resilience. The cyberattack on the National Health Service (NHS) in the United Kingdom in 2017 (WannaCry). The attack disrupted the functioning of medical institutions, highlighting the need for reliable organizational response and recovery plans, as well as effective information and data protection systems (House of Commons Committee of Public Accounts, 2018, April 18).

Social and Economic Resilience. The "Yellow Vests" protests in France that began in 2018 due to economic and social issues. Distrust in government reforms and social unrest negatively affected the economy and the resilience of infrastructure, emphasizing the importance of citizen trust and the stability of social systems in ensuring economic resilience (Cigainero, 2018, December 3).

Environmental and Physical Resilience. The Italian city of Venice frequently faces flooding issues due to rising sea levels and climate change. The city's infrastructure, including historic buildings and transport systems, is constantly at risk of damage. Strengthening the physical resilience of infrastructure and developing ecological solutions (such as the MOSE system for flood protection) are critical for maintaining Venice's functionality (Bonjour Venise, 2024, February 24).

Functional and Informational Resilience. Under martial law, Ukraine experienced a series of large-scale cyberattacks that disrupted the functioning of government and financial systems. The cyberattacks revealed vulnerabilities in information systems and communication networks and demonstrated that insufficient IT protection can seriously impact organizations' ability to maintain continuous operations.

Organizational and Social Resilience. An example of this interaction is the response to the COVID-19 pandemic in the EU. Organizational resilience, including effective coordination among member states and health authorities, was key to ensuring social resilience, building citizen trust in vaccination, and implementing quarantine (epidemiological) measures (Council of the EU and the European Council, n. d.)

These examples illustrate how different aspects of resilience interact and influence one another, emphasizing the importance of a comprehensive approach by governments to ensure the resilience of critical infrastructure facilities.

Conclusions

The protection of critical infrastructure and the assurance of the resilience of vital facilities are essential for modern society. Without reliable energy supply, safe drinking water, medical services, banking and financial services, or predictable transportation, our way of life would be impossible.

Critical infrastructure provides important functions for the state, and infrastructure sectors are interconnected. An attack on a single facility within the network will affect other facilities and networks. The degree of interdependence between defence and infrastructure is high and complex. The destruction or damage of even one facility that is part of critical infrastructure can have tragic consequences.

Institutional assurance of critical infrastructure resilience is a system of organizational, legal, and administrative mechanisms that ensure the reliable functioning and protection of critical infrastructure from threats and challenges. Its main elements include: legislative and regulatory frameworks; management authorities; critical infrastructure operators; risk management and emergency response systems; personnel training and education; and financial support for critical infrastructure.

The approaches to ensuring critical infrastructure resilience in the EU, NATO, and Ukraine share common features but differ due to their specific functions and objectives. The EU focuses on developing regulatory

frameworks and creating integrated protection systems aimed at safeguarding the civilian population, economy, and environment. NATO concentrates on ensuring the resilience of infrastructure necessary for military operations and collective defence, with an emphasis on cybersecurity, energy security, and transportation corridors.

Ukraine, due to the conditions of war, prioritizes the rapid restoration of damaged infrastructure, protection against physical and cyberattacks, and integration with partner systems. A key difference is that while the EU and NATO operate in peacetime, Ukraine must ensure infrastructure resilience during active hostilities. Nevertheless, all three systems recognize the importance of collaboration between the public and private sectors to achieve this goal.

The main determinants of the resilience of critical infrastructure entities include: physical resilience, functional resilience, organizational resilience, informational resilience, social resilience, economic resilience, and environmental resilience. These determinants are interconnected and collectively impact the ability of critical infrastructure entities to ensure continuous operation in crisis situations and to sustain economy in the crisis situations that confirms the article hypothesis.

Currently, critical infrastructure of Ukraine is undergoing a stress test for resilience. Our further scientific research will be dedicated to assessing the degree of its resilience in wartime.

REFERENCE/СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Becker, J., Duda, M., & Lute, D. (2022). From context to concept: history and strategic environment for NATO's 2022 strategic concept. *Defence Studies, 22*(3), 489–496. https://doi.org/10.1080/14702436.2022.2082959

Bonjour Venise. (2024, February 24). *Flooding in Venice: Current causes and preventive measures*. https://bonjourvenise.fr/en/flooding-venice

Cigainero, J. (2018, December 3). Who Are France's Yellow Vest Protesters, And What Do They Want? *NPR.* https://www.npr.org/2018/12/03/672862353/who-are-frances-yellow-vest-protesters-and-what-do-they-want

Council of the EU and the European Council. (n. d.). *The EU's response to the COVID-19 pandemic.* https://www.consilium.europa.eu/en/policies/coronavirus-pandemic/

EEAS. Delegation of the European Union to Ukraine. (2024, May 22). *EU and Nefco initiative makes significant progress in rebuilding Ukraine's critical infrastructure*. https://www.eeas.europa.eu/delegations/ukraine/eu-and-nefco-initiative-makes-significant-progress-rebuilding-ukraine's-critical-infrastructure_en?s=232

European Commission. (2024, September 23). *Critical infrastructure resilience at EU-level.* https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilienceen.

Horvits, E. (2024). *Fortifying the Resilience of our Critical Infrastructure.* https://www.linkedin.com/pulse/fortifying-resilience-our-critical-infrastructure-eric-horvitz-gq84c

House of Commons Committee of Public Accounts. (2018, April 18). Cyber-attack on the NHS. *Thirty-Second Report of Session 2017–19*. https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/787/787.pdf

Khrapkina, V. V. (2024). Mechanisms for Ensuring the Resilience of Critical Infrastructure: European Experience. In V. V. Khrapkina, N. V. Trushkina, (Eds.), *Management of Innovative Development of Socio-Economic Systems*, Kyiv-Mohyla Academy (6.3), 613–626. https://ekmair.ukma.edu.ua/server/api/core/bitstreams/956affad-5103-4f4b-b19f-cbbe18e4c839/content	Храпкіна, В. В. (2024). Механізми забезпечення стійкості критичної інфраструктури: європейський досвід. У Храпкіна В. В., Трушкіна Н. В. (Ред.), *Управління інноваційним розвитком соціально-економічних систем.* Національний університет "Києво-Могилянська академія". Києво-Могилянська академія, (6.3), 613–626. https://ekmair.ukma.edu.ua/server/api/core/bitstreams/956affad-5103-4f4b-b19f-cbbe18e4c839/content
Kyiv Post. (2024, February 19). Critical Infrastructure Objects of Ukraine: Everything You Need to Know. https://www.kyivpost.com/uk/post/28283	Kyiv Post. (2024, 19 лютого). Об'єкти критичної інфраструктури України: все, що варто знати. https://www.kyivpost.com/uk/post/28283

Lagutin, V., Boiko, A., & Shkuropadska, D. (2020). Institutional conditions for ensuring resilience of national economy: on the example of Ukraine. Latvia. *Baltic Journal of Economic Studies, 6*(3), 76–86.

Law of Ukraine "On Critical Infrastructure" № 1882-IX (2024, September 21). https://zakon.rada.gov.ua/laws/show/1882-20#Text	Закон України "Про критичну інфраструктуру" № 1882-IX (2024, 21 вересня). https://zakon.rada.gov.ua/laws/show/1882-20#Text

Lebedeva, L., & Shkuropadska, D. (2024a). Resilience of transport logistics in EU and Ukraine. *Foreign trade: economics, finance, law, 4*(135), 108–127. https://doi.org/10.31617/3.2024(135)07

Lebedeva, L., & Shkuropadska, D. (2024b). Determinants of energy system resilience. *Scientia fructuosa*, *3*(155), 23–41. https://doi.org/10.31617/1.2024(155)02

Lebedeva, L., & Shkuropadska, D. (2024c). Resilience of EU Healthcare Systems. *Foreign Trade: Economics, Finance, Law*, *2*(133), 120–133. https://doi.org/10.31617/3.2024(133)07

Melnychuk, O. (2021). Current Issues of Public Policy on Critical Infrastructure Resilience: Status and Prospects for its Implementation in Ukraine. *Mechanisms of Public Administration*, (26), 90–112. http://taais.oridu.odessa.ua/article/view/239031	Мельничук, О. (2021). Актуальні питання публічної політики стійкості критичної інфраструктури: стан та перспективи її впровадження в Україні. *Mechanisms of public administration,* (26), 90–112. http://taais.oridu.odessa.ua/article/view/239031

Mukherjee, M., Abhinay, K., Rahman, M. M., Yangdhen, S., Sen, S., Adhikari, B. R., ... & Shaw, R. (2023). Extent and evaluation of critical infrastructure, the status of resilience and its future dimensions in South Asia. *Progress in Disaster Science*, (17), 100275.

NATO Summit Guide. (2016, July). *Warsaw, 8-9 July.* https://www.ulib.sk/files/sk/depozitna-kniznica-nato/fondy/monografie/warsaw-summit-guide_2016eng.pdf

Ninković, V. (2021). Critical infrastructure resilience – national approaches in the United States of America, the United Kingdom and Australia. *Collected Papers of the Faculty of Law in Novi Sad, University in Novi Sad*, *LV*(4), 1205–1225, https://doi.org/10.5937/zrpfns55-30333	Ninković, V. (2021) Critical infrastructure resilience – national approaches in the United States of America, the United Kingdom and Australia. *Collected Papers of the Faculty of Law in Novi Sad, University in Novi Sad*, *LV*(4), 1205–1225, https://doi.org/10.5937/zrpfns55-30333
NISS. (2013, December 9). European Experience in Developing a Critical Infrastructure Protection System: Lessons for Ukraine". *Analytical Note. National Institute for Strategic Studies. National institute for strategic studies.* https://www.niss.gov.ua/doslidzhennya/nacionalna-bezpeka/evropeyskiy-dosvid-rozbudovi-sistemi-zakhistu-kritichnoi	НІСД. (2013, 9 грудня). Європейський досвід розбудови системи захисту критичної інфраструктури: уроки для України" *Аналітична записка. National institute for strategic studies*. https://www.niss.gov.ua/doslidzhennya/nacionalna-bezpeka/evropeyskiy-dosvid-rozbudovi-sistemi-zakhistu-kritichnoi

OECD. (2019, April 17). *OECD Reviews of Risk Management Policies. Good governance for critical infrastructure resilience.* https://doi.org/10.1787/02f0e5a0-en

Osei-Kyei, R., Melo Almeida, L., Ampratwum, G., & Tam, V. (2022). Systematic Review of Critical Infrastructure Resilience Indicators. *Construction Innovation Information, Process, Management 23*(4). https://doi.org/10.1108/CI-03-2021-0047

PwC. (n. d.). *Critical Entities Resilience Directive: Why it is relevant to you*. https://www.pwc.com/ee/en/services/advisory-services/crisis-management/critical-entities-resilience-directive.html

Roepke, W.-D., & Thankey, H. (2019, February 27). Resilience is the first line of defense. NATO Review. https://www.nato.int/docu/review/uk/articles/2019/02/27/stjkst-persha-lnya-oboroni/index.html

Roepke, W.-D., & Thankey, H. (2019, 27 лютого). *Стійкість – перша лінія оборони. NATO Review.* https://www.nato.int/docu/review/uk/articles/2019/02/27/stjkst-persha-lnya-oboroni/index.html

Shelest, H. (2021). *NATO and Ukraine's resilience concept.* https://prismua.org/nato_ukraine

Шелест, Г. (2021). *Концепція стійкості НАТО та України*. https://prismua.org/nato_ukraine

Shkuropadska, D., Lebedeva, L., Shtunder, I., Nikolaiets, K., Ozhelevskaya, T., & Sokolovska, I. (2024). Food Resilience in Ukraine During Martial Law. *Financial and Credit Activity Problems of Theory and Practice, 5*(58), 409–420. https://doi.org/10.55643/fcaptp.5.58.2024.4503

Umantsiv, Yu., & Shkuropadska, D. (2023). National resilience of Ukraine under the Martial Law. *Scientia fructuosa*, (5), 4–19. https://doi.org/10.31617/1.2023(151)01

Witting, V. (2023). *Germany's Ahr Valley flood survivors reflect on the rebuild. DW*. https://www.dw.com/en/germanys-ahr-valley-flood-survivors-reflect-on-the-rebuild/a-66178329

Yang, Z., Barroca, B., Laffréchine, K., Weppe, A., Bony-Dandrieux, A., & Daclin, N. (2023). A multi-criteria framework for critical infrastructure systems resilience. *International Journal of Critical Infrastructure Protection,* (42), 100616, https://doi.org/10.1016/j.ijcip.2023.100616

Conflict of interest. The authors certify that don't they have any financial or non-financial interest in the subject matter or materials discussed in this manuscript; the authors have no association with state bodies, any organizations or commercial entities having a financial interest in or financial conflict with the subject matter or research presented in the manuscript. Given that one of the authors is affiliated with the institution that publishes this journal, which may cause potential conflict or suspicion of bias and therefore the final decision to publish this article (including the reviewers and editors) is made by the members of the Editorial Board who are not the employees of this institution.

The preparation of the article was financed within the Erasmus+ Jean Monnet project: 101083497 — EUERP — ERASMUS-JMO-2022-HEI-TCH-RSCH "EU Economic Resilience Policy".

The contribution of the authors is equal

Shkuropadska, D., Lebedeva, L., Gonçalves, J. Institutional framework for the resilience of critical infrastructure of EU, NATO countries and Ukraine. *Scientia fructuosa*. 2025. № 1. P. 45–60. https://doi.org/10.31617/1.2025(159)03

Received by the editorial office 06.01.2025.
Accepted for printing 15.01.2025.
Published online 17.02.2025.