Working together
www.rcis.ro

Revista de Cercetare si Interventie Sociala

ISSN: 1583-3410 (print), ISSN: 1584-5397 (electronic)

RISK-BASED MODEL OF PUBLIC MANAGEMENT OF CRITICAL INFRASTRUCTURE RESILIENCE IN THE FACE OF MULTIDIMENSIONAL THREATS TO NATIONAL SECURITY

Serhii BIELAI, Mykhailo PUZYROV, Vadym YEVSIEIEV, Kyrylo TKACHENKO, Andrii HOLOVNIA

Revista de cercetare și intervenție socială, 2026, vol. 94, pp. 136-158

https://doi.org/10.33788/rcis.94.8

Published by:
Expert Projects Publishing House

expert projects
publishing

On behalf of:
„Alexandru Ioan Cuza" University,
Department of Sociology and Social Work
and
HoltIS Association

Risk-Based Model of Public Management of Critical Infrastructure Resilience in the Face of Multidimensional Threats to National Security

Serhii BIELAI[1], Mykhailo PUZYROV[2], Vadym YEVSIEIEV[3], Kyrylo TKACHENKO[4], Andrii HOLOVNIA[5]

Abstract

The article is devoted to the development and empirical approbation of a risk-based model of public management of critical infrastructure resilience in the face of multidimensional threats to national security. On the example of the energy sector of Ukraine, the impact of military threats on the functioning of critical infrastructure, the role of state institutions and international assistance in ensuring its resilience is studied. The empirical basis of the study is open data from the Energy Map analytical platform, including three sets: massive strikes on energy facilities, the use of power supply restrictions, and international aid. The data is aggregated to the monthly level for the period 2022-2026. For a comprehensive assessment of resilience, the Integral Index of Critical Infrastructure Resilience is

[1] Center for Organization and Coordination of Scientific and Innovative Activities of the National Academy of the National Guard of Ukraine, Kharkiv, UKRAINE. E-mail: belwz3@ukr.net, ORCID: http://orcid.org/0000-0002-8627-0057

[2] Department of Legal Disciplines at Educational and Scientific Institute of Personnel Management of the National Academy of the National Guard of Ukraine, Kharkiv, UKRAINE. E-mail: mpuzyrov@gmail.com, ORCID: http://orcid.org/0000-0002-7814-9476

[3] Kharkiv National University of Internal Affairs, Kharkiv, UKRAINE. E-mail: ua117@ukr.net, ORCID: https//orcid.org/0000-0002-0164-2991

[4] Department of Military Communications and Informatization, National Academy of the National Guard of Ukraine, Kharkiv, Ukraine. E-mail: tkn-ngu@ukr.net, ORCID: https://orcid.org/0000-0001-7678-0363

[5] Department of Command and Staff Training, Educational and Research Institute of Professional Education, National Academy of the National Guard of Ukraine, Kharkiv, UKRAINE. E-mail: golovnijandr1@ukr.net, ORCID: https://orcid.org/0000-0001-9188-0055

proposed, which integrates three components: the level of threats (Threat Index), the consequences of risk implementation (Consequences Index) and the recovery capacity (Recovery Index). The results of the analysis revealed the cyclical nature of the impact of threats on the power system, a high level of correlation between the intensity of attacks, power outages and the volume of assistance. It is shown that international support plays a key role in compensating for losses, but it is mainly reactive. The dynamics of the Integral Index of Critical Infrastructure Resilience demonstrate the adaptive resilience of the system, which manifests itself in cyclical recovery from periods of crisis, although overall resilience remains vulnerable to intense attacks. The proposed model confirms the transition from traditional risk management to holistic, adaptive governance. The results of the study are of theoretical importance for the development of dynamic resilience concepts and practical value for improving the policy of critical infrastructure protection in the face of military and hybrid threats. Prospects for further research are related to the extension of the model to other sectors and the integration of social indicators.

Keywords: risk-based management; critical infrastructure resilience; energy security; multidimensional threats; Integral Index of Critical Infrastructure Resilience; international aid.

Introduction

Modern challenges to national security, including full-scale war and hybrid threats, actualize the need for effective models of public management of critical infrastructure resilience. Ukraine's energy sector, which has been subjected to systemic massive attacks, has become a critical test for state institutions, demonstrating both the vulnerability and adaptive potential of society. Under these conditions, traditional approaches to risk management are insufficient, since they do not take into account the full cycle of risk – from threat formation through the implementation of consequences to system recovery and transformation.

The purpose of the study is to develop and empirically test a risk-based model of public management of critical infrastructure resilience in the face of multidimensional threats to national security. The relevance of the work is due to the need to move from a reactive response to proactive, integrated management, which combines prevention, mitigation and strengthening of recovery capacity. Such a transformation is in line with the current trends in the development of digital and innovative public administration, within which strategic decisions are increasingly based on the use of data, adaptive governance mechanisms and cross-sectoral interaction (Buryk, 2025).

The scientific novelty lies in the empirical construction of a risk-based model based on the unique data of the Energy Map platform, covering the period 2022–

2026, as well as in the development of an integral index that allows you to quantify the balance between threats, consequences and recovery. The practical significance of the study lies in providing tools for public administration bodies that can be used to monitor resilience, make operational decisions and strategic recovery planning.

Literature Review

Modern public critical infrastructure resilience management (further – CI) in the context of multidimensional threats to national security has evolved from traditional risk management to holistic, risk-oriented, and adaptive governance. This transition also involves the development of mechanisms for data formalization and analytical support of management decisions, which is an important condition for effective management of the socio-economic security of the state (Buryk *et al*., 2019). This transformation reflects an understanding of resilience not as a static property, but as a system's dynamic ability to anticipate, absorb, recover, and adapt to crises, particularly military crises (Boin & van Eeten, 2013; Linkov & Trump, 2019).

At the conceptual level, frameworks that integrate the three interrelated components of risk: threat, consequences and regenerative capacity are key. Bruneau *et al*. (2003) proposed a four-dimensional model of resilience (technical, organizational, social, economic), which serves as a basis for evaluating infrastructure systems. Holling (1973) introduced the distinction between engineering resilience (rapid return to equilibrium) and ecological resilience (ability to transform), which is especially important for energy systems in conditions of prolonged war. Kaplan and Mikes (2012) developed a risk management framework, emphasizing preventive, detective, and mitigative controls in the public sector.

In the context of hybrid and military threats, the literature emphasizes the need for multi-level governance. Ansell *et al*. (2021) analyze COVID-19 as a "turbulent problem" that requires robust governance with a focus on coordination between the state, private sector and international partners – an approach that is directly applicable to the Ukrainian experience. Cutter *et al*. (2010) developed disaster resilience indicators that take into account baseline conditions and community resilience, complementing the techno-economic metrics with a social dimension.

Specifically for Ukraine and the energy sector, empirical studies in recent years record the lessons of resilience during a full-scale invasion. Aebi *et al*. (2024) in the Risk and Resilience report take a detailed look at the resilience of energy, transport, and communications, highlighting the role of 2021 legislation, coordination headquarters, and international assistance in mitigating the effects of attacks. Maznyk (2026) conceptualizes spillover risks for Europe by analyzing the cross-border effects of the destruction of the Ukrainian energy sector and the need for an integrated shock probability – vulnerability – recovery capacity framework. In particular, the economic aspects of public administration and local

self-government in the context of ensuring national security are considered in the work of Zayats *et al*. (2024), where the relationship between administrative mechanisms and the resilience of critical sectors of the economy is emphasized.

Rimutis (2024) assesses the extent of damage and resilience of the power system, emphasizing the role of generators, decentralization, and international support as stabilizing factors. Kichata (2025) proposes a risk assessment methodology for critical infrastructure facilities using the example of water treatment complexes, emphasizing the integration of war risks. Mitoulis *et al*. (2023) developed a conflict-resilience framework for post-war recovery, combining technical recovery with peacebuilding.

The European and global context complements national cases. EU Directive 2022/2557 (European Union, 2022) sets standards for resilience critical entities, with a focus on stress-testing and preparedness in the energy sector. Thistlethwaite and Henstra (2026) analyzes policy instruments for cybersecurity of critical infrastructure, considering hybrid threats. Wells *et al*. (2022) model intersystem resilience, demonstrating how interdependence amplifies vulnerability.

Recent works highlight institutional transformations. Strahnitskyi (2024) examines the state policy of CI protection in Ukraine. Zahorna (2025) focuses on the economic consequences of destruction and the need for public-private partnerships for modernization. Georgescu (2025) proposes Critical Infrastructure Protection of the conflict in Ukraine, recommending hardening, rerouting, and post-ceasefire reconstruction.

Thus, the literature forms a scientific chain: from the theoretical foundations of resilience through risk-oriented governance to applied military cases and policy recommendations. The study fills a gap in the quantification of risk-based models specifically for the Ukrainian energy sector in the face of long-term multidimensional threats, combining empiricism with a humanistic focus on societal resilience and restoration of human potential.

Methodology

The study is based on a quantitative analysis of open data from the analytical platform Energy Map (DiXi Group, 2026). Three main data sets were used: information on massive strikes on critical infrastructure (Energy Map, 2026a), the application of measures to limit electricity consumption (Energy Map, 2026b), and international assistance to the Ukrainian energy sector (Energy Map, 2026c). These kits cover the period from 2022 to 2026 and allow you to trace the full cycle of risk – from the emergence of a threat through its consequences to the restoration of the system.

The primary data was aggregated to the monthly level. Aggregation included summing up quantitative indicators (number of weapons, hours of restrictions,

amounts of assistance) and counting events (attacks, cases of assistance) within each month. For data on international assistance, coding of categorical variables and conjugation tables were constructed to analyze the structure of support.

Due to the significant asymmetry of the distributions and the presence of extreme values, all quantitative series have undergone a logarithmic transformation. To assess the relationships between the level of threats, consequences and recovery, the analysis of lag cross-correlation with time shifts from -5 to 5 months was used.

The Integrated Critical Infrastructure Resilience Index (IICIR) is built on the basis of three components: the Threat Index, the Consequences Index, and the Recovery Index. Each component is normalized using the minimum-maximum method based on logarithmic series. The index was calculated as a weighted combination of components, where the recovery capacity has a positive contribution, and the threats and consequences have a negative contribution. This made it possible to obtain a comprehensive assessment of the stability of the system in dynamics.

All calculations and visualizations are performed using IBM SPSS Statistics 27 software. This approach ensures objectivity, reproducibility of results and compliance with the standards of modern research in the field of risk-based public administration and critical infrastructure resilience.

Results

As part of the study of the risk-based model of public management of the resilience of critical infrastructure in the face of multidimensional threats to national security, an empirical base was formed, which allows assessing not only the scale of external impact on the energy system of Ukraine, but also the ability of state institutions to ensure its functioning and recovery. According to the modern approach to critical infrastructure resilience management, risk assessment should take into account three interrelated components: the level of threat, the consequences of its implementation, and the adaptive capacity of the system to recover (Boin & van Eeten, 2013; Linkov & Trump, 2019). That is why the study has formed a system of indicators that reflects not a separate aspect of the crisis, but the full cycle of risk emergence and overcoming: from the moment of threat formation to the restoration of the functionality of critical infrastructure.

The information basis of the study was open data of the analytical platform Energy Map, which specializes in collecting, systematizing and disseminating data on the functioning of the energy sector of Ukraine. The resource was created as a tool for ensuring transparency of the energy sector and the formation of an open database for analytical and research purposes (DiXi Group, 2026). Unlike

traditional energy statistical resources, the Energy Map contains not only economic and technical indicators of the functioning of the energy sector, but also specialized data sets formed in the context of a full-scale war, reflecting the impact of military threats on Ukraine's critical infrastructure.

For the purposes of this study, three Energy Map datasets are of particular importance: information on massive strikes on Ukraine's critical infrastructure, information on the application of measures to limit electricity consumption, and information on partners' assistance to the Ukrainian energy sector. Their association corresponds to the logic of risk-based management, as it allows you to trace the cause-and-effect chain: the military threat → disruption of the functioning of the energy system → the mobilization of resources for recovery.

The first block of data was formed on the basis of the set "Information on Massive Strikes on Critical Infrastructure of Ukraine" (Energy Map, 2026a). This kit contains information on large-scale missile and drone attacks on Ukraine's energy facilities and covers the period from September 11, 2022 to April 1, 2026. An important feature of this set is that it includes massive attacks that had the potential to systematically affect the functioning of the energy system. The data is based on official reports from the Ministry of Energy of Ukraine, NPC Ukrenergo and information from the Air Force of the Armed Forces of Ukraine on the number of weapons used and destroyed.

Within the framework of the model, this block is considered as a characteristic of exogenous risk, i.e. an external influence that does not depend on the functioning of the energy system itself. Two indicators were chosen to quantitatively measure the threat level: Number of weapons used, units and Number of weapons shot down, units. The first indicator characterizes the intensity of the attack and reflects the scale of the potential load on critical infrastructure. The second indicator is included in the model as a characteristic of the effectiveness of the protective component of the risk management system, since it demonstrates the ability of the state to reduce the consequences of the threat implementation. The results of aggregation of these indicators by monthly periods are shown in Figure 1.

The results of aggregation of indicators of massive attacks on the energy infrastructure of Ukraine showed a significant transformation in the nature of threats during the period under study. In total, in the period from September 2022 to March 2026, 231 massive attacks on energy infrastructure facilities were recorded, of which 171 were carried out using missile weapons and 60 using unmanned aerial vehicles. The total number of weapons used was 18,032 units, of which 14,958 were destroyed by air defense forces.

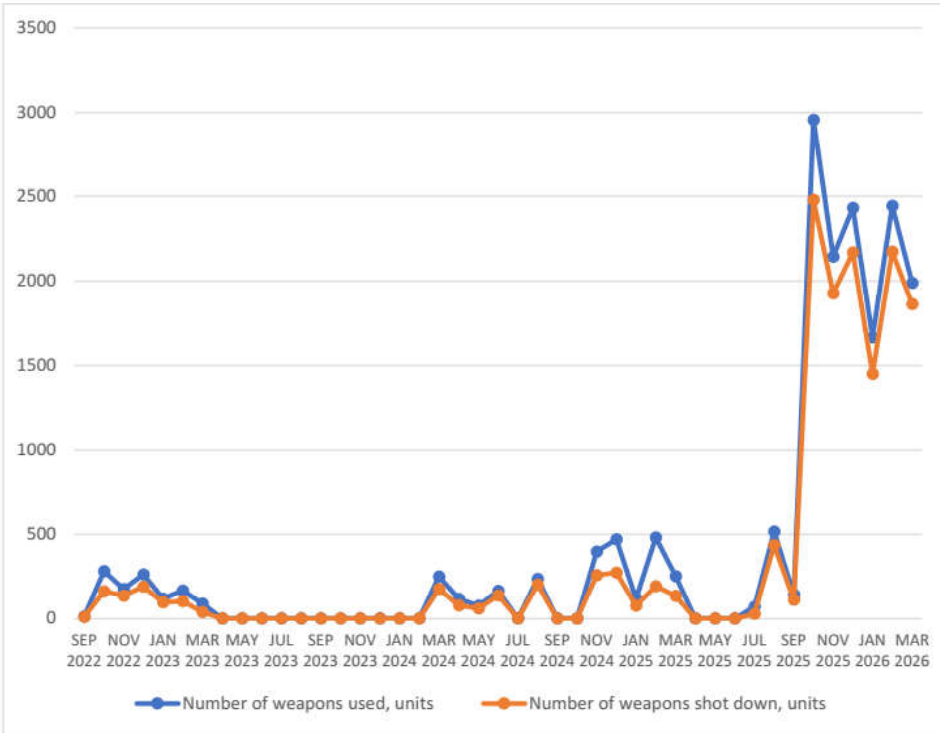

Figure 1. Dynamics of the use and neutralization of weapons of destruction against the energy infrastructure of Ukraine (September 2022 – March 2026)
Source: Compiled by the authors based on Energy Map (2026a)

The analysis of time dynamics allows us to distinguish several stages of changes in the intensity of threats. The first stage covers the period from September 2022 to March 2023 and is characterized by the formation of the practice of systemic strikes on energy infrastructure. It was during this period that the first waves of massive attacks were observed, during which the number of weapons used ranged from 89 to 282 units per month. The highest intensity was recorded in October 2022 (282 units) and December 2022 (263 units), which coincided with the beginning of large-scale use of attacks as a tool to destabilize the functioning of Ukraine's energy system.

The second stage covers the period from April 2023 to February 2024 and is characterized by the absence of massive attacks on energy infrastructure in the sample. This situation does not indicate the absence of threats in general, but reflects a change in the nature of hostilities and the absence of recorded large-scale campaigns that met the criteria for inclusion in the Energy Map dataset. During

this period, the public administration system was able to focus resources on the restoration of damaged facilities and increasing the security of the energy sector.

The third stage began in the spring of 2024 and was characterized by the resumption of systemic strikes on energy infrastructure. In March-June 2024, the number of used weapons ranged from 76 to 250 units per month. At the same time, compared to the 2022-2023 campaign. There was an increase in the share of destroyed targets, which may indicate a strengthening of air defense capabilities and an increase in the effectiveness of interagency coordination in the field of critical infrastructure protection.

The most significant changes were recorded at the fourth stage, which covers the second half of 2025 and the first quarter of 2026. If in August 2025 517 weapons were used, then in October 2025 their number increased to 2957 units, which is more than five times higher than the indicators of previous waves of attacks. The high level of threats also persisted in November and December 2025, as well as in January–March 2026, when the monthly number of weapons used exceeded 1600 units.

Special attention should be paid to the change in the structure of attacks. If missile strikes dominated at the initial stages, then during 2025-2026. The role of unmanned aerial vehicles has increased significantly. In total, 60 massive attacks using UAVs were recorded in the sample, with the highest concentration occurring during the last observation period (Figure 2). This trend reflects a change in tactics for damaging critical infrastructure and complicates the task of ensuring its resilience due to the need to counter a large number of relatively cheap weapons.

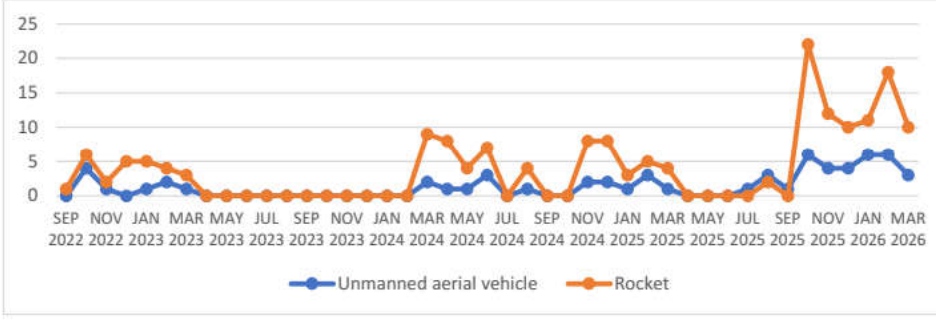

Figure 2. Dynamics of massive attacks on Ukraine's energy infrastructure (September 2022 – March 2026)

Source: Compiled by the authors based on Energy Map (2026a)

At the same time, the analysis of the ratio between the number of used and destroyed weapons demonstrates a gradual increase in the effectiveness of the threat counteraction system. If at the beginning of the study period the share of neutralized targets was significantly lower (about 65%), then at the end of the

period it exceeded 85%. From the standpoint of risk-based management, this indicates an increase in the adaptive capacity of the public administration system and its ability to compensate for the increase in the intensity of external threats through the development of critical infrastructure protection mechanisms. At the same time, the scale of attacks in 2025–2026. show that even a high level of neutralization of goals does not eliminate the risk of systemic disruptions in the functioning of the energy sector, which requires further strengthening of institutional and organizational mechanisms for ensuring resilience.

The second block of indicators is formed on the basis of the dataset "Information on the application of measures to limit electricity consumption" (Energy Map, 2026b). This set covers the period from January 1, 2023 to April 1, 2026 and contains information on the application of hourly power outage schedules by the transmission system operator NPC Ukrenergo. The dataset covers outages that were applied on a large scale - throughout the country or in a significant number of regions. Cases of introduction of exceptions within 1-3 regions are not taken into account. The peculiarity of this set is its focus not on the fact of damage to the infrastructure, but on the end result of the risk realization – the loss of the ability of the power system to ensure uninterrupted supply of electricity to consumers.

In the context of the proposed model, this block characterizes the functional stability of critical infrastructure. If the first block of indicators reflects the strength of external influence, then outage indicators demonstrate the actual ability of the system to maintain basic functions in a crisis. For the analysis, variables were used regarding the fact of introduction of restrictions on electricity consumption and the number of hours the system was in the restriction mode.

After converting the primary data into the format of monthly observations, the results are obtained, visualized in Figure 3.

Figure 3. Dynamics of the application of electricity supply restrictions in 2023–2026 (hours per month in Ukraine)

Source: Compiled by the authors based on Energy Map (2026b)

Dynamics of the application of electricity supply restrictions in Ukraine during 2023–2026 (Figure 3) demonstrates the uneven nature of the impact of military threats on the functioning of energy infrastructure. For most of 2023 and early 2024, large-scale restrictions on electricity consumption were practically not applied, which indicated a relative stabilization of the energy system after the 2022-2023 heating season and the implementation of restoration measures.

The first significant surge in the duration of outages was recorded in May-July 2024. It was during this period that the resumption of massive strikes on energy infrastructure led to a shortage of generating capacity and the need to apply large-scale restrictions on electricity supply. The indicator reached its highest values in June and July 2024, which indicates the direct impact of the destruction of energy facilities on the functioning of the power system.

The second, longer crisis period began in the fall of 2025. If in October the blackouts were localized, then in November-February there was a sharp increase in the number of hours of restrictions. Peak values were recorded in December 2025, January and February 2026, when virtually the entire monthly fund of hours was characterized by the use of certain restrictive measures. This situation coincided with the period of the highest intensity of massive missile and drone attacks on energy infrastructure, which indicates the cumulative effect of damage and an increase in the load on the critical infrastructure resilience management system.

At the same time, already in March 2026, there is a significant reduction in the duration of outages, which may indicate a partial restoration of damaged capacities, adaptation of the operating modes of the power system, and the effectiveness of public administration and international support measures in the field of energy infrastructure restoration. In general, these dynamics confirm that the scale of power supply restrictions is determined not only by the intensity of external threats, but also by the ability of the public administration system to ensure rapid restoration and maintenance of the functional stability of critical infrastructure.

After logarithmic transformation of the series (to reduce asymmetry and the influence of extreme values), a lag cross-correlation analysis was performed. The results showed a very strong positive relationship between the number of massive attacks and the number of hours of power supply restrictions ($r = 0.952$ at a lag of 0 and $r = 0.696$ at a lag of +1). The obtained coefficients indicate that massive attacks in almost real time lead to a significant increase in power deficit and the need to apply hourly outage schedules. Such a high level of correlation confirms the critical vulnerability of the energy infrastructure to military threats and indicates the limited buffer capabilities of the system even when public administration measures are applied.

The third block of indicators is formed on the basis of the dataset “Information on the provision of assistance by partners to the Ukrainian energy sector” (Energy Map, 2026c). This kit covers the period from March 14, 2022 to April 1, 2026 and contains information on materials, equipment, financing and other forms of support

received from international partners to restore Ukraine's energy infrastructure. The sources of information are official reports of ministries, state administrations, international organizations and representative offices of partner countries.

The inclusion of this block in the model is due to the fact that the modern understanding of the resilience of critical infrastructure implies not only the ability to counter threats, but also the ability to quickly restore functionality after their implementation. Thus, assistance is considered as an indicator of the adaptive and restorative capacity of the public administration system.

After encoding the categorical variables and aggregating the data, the structure of assistance given in the Table 1 was obtained.

Table 1. Month _Year* Type of Assistance Crosstabulation

	Type of assistance											Total
	Consultancy	Credit	Materials	Equipment	Fuel	Loan	Software	Raw materials	Cooperation	Equipment	Funding	
MAR 2022	0	0	0	1	0	0	0	0	0	0	0	1
AUG 2022	0	0	0	1	1	0	0	0	0	0	0	2
SEP 2022	0	0	1	6	0	0	0	0	0	0	0	7
OCT 2022	0	0	1	7	0	1	0	0	2	0	6	17
NOV 2022	0	0	0	29	0	0	0	0	2	0	16	47
DEC 2022	0	0	2	55	1	2	0	0	5	0	19	84
JAN 2023	0	0	2	62	2	0	0	0	2	0	7	75
FEB 2023	0	0	0	75	1	0	0	1	2	0	7	86
MAR 2023	0	0	1	59	2	0	0	0	2	0	1	65
APR 2023	0	0	0	39	0	0	0	0	1	0	4	44
MAY 2023	0	0	1	22	0	0	0	1	0	0	1	25
JUN 2023	0	0	0	32	0	1	0	0	3	2	15	53
JUL 2023	2	0	0	27	0	0	0	0	3	0	6	38
AUG 2023	0	0	0	13	0	0	0	0	0	0	3	16
SEP 2023	0	0	0	4	0	0	0	0	0	0	2	6
OCT 2023	0	0	0	3	0	0	0	0	0	0	1	4
NOV 2023	0	0	0	11	1	2	0	0	0	0	6	20
DEC 2023	0	0	1	1	0	1	0	0	0	0	5	8
JAN 2024	0	0	0	5	0	0	0	0	0	0	0	5

FEB 2024	0	0	0	8	0	1	0	0	0	0	0	9
MAR 2024	0	0	0	4	0	0	0	0	0	0	1	5
APR 2024	0	0	1	16	0	0	0	0	0	0	1	18
MAY 2024	0	0	0	3	0	0	0	0	2	0	7	12
JUN 2024	0	0	2	12	0	3	0	0	0	0	7	24
JUL 2024	0	0	0	6	0	2	0	0	0	0	0	8
AUG 2024	0	0	0	3	0	1	0	0	0	0	1	5
SEP 2024	0	0	0	1	0	0	0	0	0	0	10	11
OCT 2024	0	0	0	11	0	0	0	0	1	0	3	15
NOV 2024	0	0	0	30	1	0	0	0	0	0	2	33
DEC 2024	0	0	0	18	0	0	1	0	0	0	6	25
JAN 2025	0	0	0	39	0	0	0	0	0	0	2	41
FEB 2025	0	0	0	23	0	0	0	0	0	0	0	23
MAR 2025	0	0	0	9	0	0	0	0	0	0	1	10
APR 2025	0	0	0	8	0	0	0	0	0	0	1	9
MAY 2025	0	0	0	7	0	0	0	0	0	0	1	8
JUN 2025	0	0	0	21	0	0	0	0	0	0	4	25
JUL 2025	0	0	0	15	0	0	0	0	0	0	11	26
AUG 2025	0	1	0	18	0	0	0	0	0	0	3	22
SEP 2025	0	0	0	14	0	0	0	0	0	0	3	17
OCT 2025	0	1	0	11	0	0	0	0	0	0	6	18
NOV 2025	0	1	0	7	0	0	0	0	0	0	4	12
DEC 2025	0	0	0	17	0	0	0	0	0	0	7	24
JAN 2026	0	1	0	62	0	0	0	0	0	1	10	74
FEB 2026	0	0	1	47	0	0	0	0	0	0	13	61
MAR 2026	0	0	0	10	1	0	0	0	0	1	3	15
Total	2	4	13	872	10	14	1	2	25	4	206	1153

The results of the analysis of international assistance to Ukraine's energy sector indicate the formation of a large-scale external support mechanism aimed at ensuring the resilience and restoration of critical infrastructure in the face of prolonged military threats (Figure 4). In the study period, 1153 cases of various types of assistance were recorded, and the total amount of documented financial support amounted to EUR 22,669.75 million.

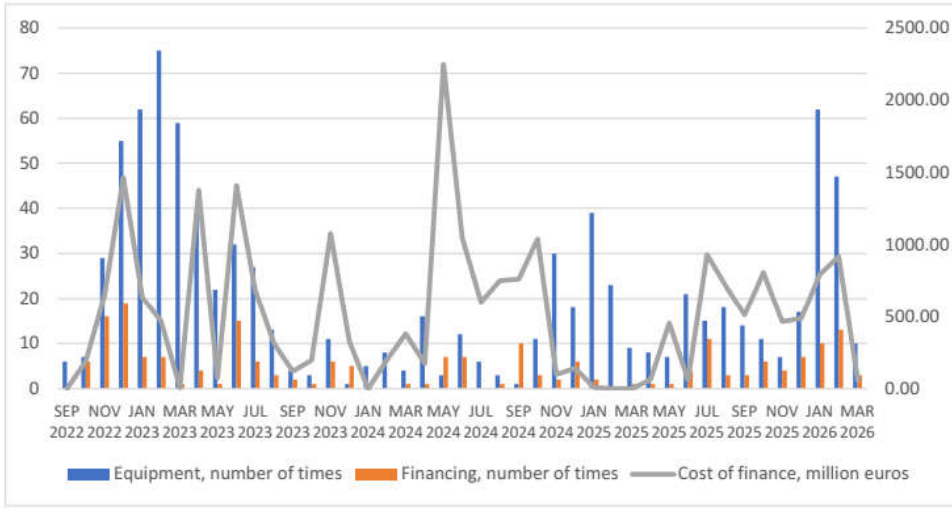

Figure 4. Dynamics of international assistance for the restoration of Ukraine's energy infrastructure in 2022–2026

Source: Compiled by the authors based on Energy Map (2026c)

Structural analysis shows that international support was focused primarily on the prompt restoration of damaged energy facilities. The largest share of all cases of assistance was the supply of equipment – 872 cases, or about 75.6% of the total number of recorded support measures. This indicates the dominance of a practical approach to the restoration of energy infrastructure, in which priority was given to transformers, generators, high-voltage equipment, components and other material and technical resources necessary to restore the functioning of the power system after damage.

The second most common type of support was direct funding, which was recorded in 206 cases. Its share was almost 18% of all cases of assistance. Other forms of support were provided much less frequently, including cooperation between organizations and institutions (25 cases), loans (14 cases), materials (13 cases), fuel (10 cases), credit resources (4 cases), equipment (4 cases), advisory support (2 cases), raw materials (2 cases) and software (1 case). Thus, the structure of assistance demonstrates the predominance of resources directly related to the physical restoration of damaged facilities and ensuring the continuity of the functioning of the energy system.

The analysis of the financial component of assistance shows significant fluctuations in its volume over time, which largely coincided with the periods of the most intense attacks on energy infrastructure. The largest amounts of funding were recorded in December 2022 (EUR 1461.71 million), April 2023 (EUR 1374.86 million), June 2023 (EUR 1408.09 million), November 2023 (EUR 1076.67

million), May 2024 (EUR 2249.4 million), June 2024 (EUR 1045.7 million) and October 2024 (EUR 1038.89 million). The concentration of significant amounts of financial resources in these periods indicates the reactive nature of international support, when the scale of assistance increased in response to the deterioration of the security situation and the increase in the need for the restoration of damaged energy capacities.

An additional analysis of the structure of donor support showed a high level of concentration of assistance among a limited number of international partners (Figure 5). The largest number of cases of support was recorded from Germany (132 cases), USAID (84), international partners in the format of joint programs and coalitions (48), Japan (46), Poland and France (33 each), the European Union and UNICEF (32 each). The vast majority of assistance was provided in the form of equipment supplies, which indicates the orientation of international support to ensure the prompt restoration of damaged energy facilities and increase the resilience of the power system. At the same time, a significant number of repeated cases of assistance by individual partners reflects not only the scale of resources involved, but also the sustainability of international support, which is an important characteristic of the adaptive and recovery capacity of the public critical infrastructure management system.

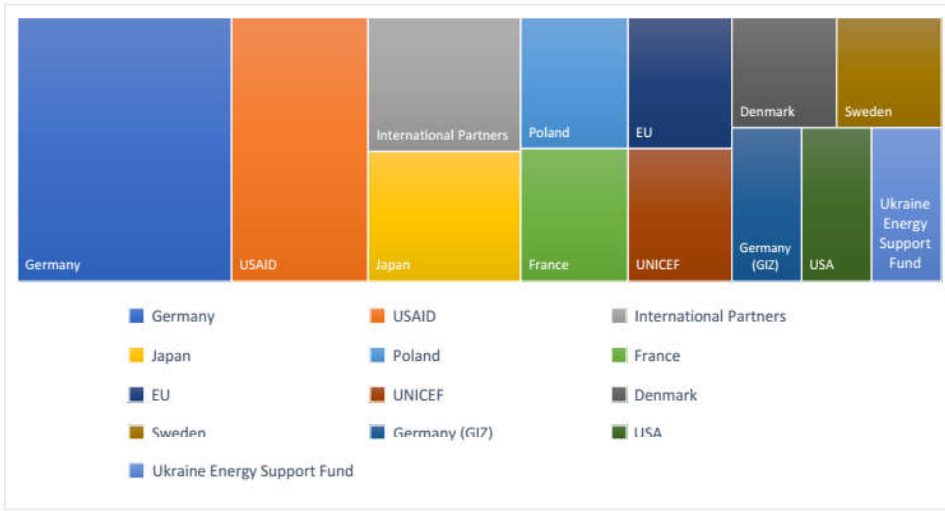

Figure 5. Structure of international assistance to the energy sector of Ukraine by donors and types of support (the most active participants)

Source: Compiled by the authors based on Energy Map (2026c)

The analysis of the lag cross-correlation between the logarithmic series of the number of weapons used and the indicators of international assistance revealed

a strong positive relationship. The maximum correlation is observed at a lag of 0: r = 0.780 with the number of aid cases and r = 0.737 with the amount of financial assistance (million euros). High correlation values are also maintained at a lag of +1 (0.663 and 0.533, respectively). The results confirm the reactive nature of international support: an increase in the intensity of massive attacks almost immediately (in the same month) leads to a significant increase in both the number of cases and the financial volume of assistance. Such a short lag indicates a relatively prompt response of international partners, but at the same time emphasizes the dependence of the critical infrastructure recovery system on external resources and the limited capacity of internal public administration mechanisms to accumulate reserves and act preventively.

The results obtained confirm that international assistance is an important element of the risk-based model of public management of critical infrastructure resilience. If the indicators of massive attacks characterize the level of threats, and the indicators of power outages reflect the consequences of the implementation of risks, then the volume and structure of international assistance demonstrate the availability of resource potential for the restoration and adaptation of the energy system. It is this component that largely determines the ability of the state to ensure the long-term stability of critical infrastructure in the face of multidimensional threats to national security.

Formation of an integral index of critical infrastructure resilience

For a comprehensive assessment of the ability of Ukraine's energy infrastructure to function in the face of multidimensional threats, the Integral Index of critical infrastructure resilience (IICIR) was formed. The need to develop such an indicator is due to the fact that the resilience of critical infrastructure cannot be adequately assessed only because of individual damage characteristics or the number of attacks. Modern approaches to resilience management consider it as a dynamic property of the system, including the ability to withstand external influences, minimize the consequences of disturbances and ensure rapid restoration of functionality (Linkov & Trump, 2019; Bruneau *et al*., 2003).

Within this study, IICIR is built on the basis of three interrelated components: (1) Threat Index (TI) – characterizes the intensity of external risk exposure; (2) Consequences Index (CI) – reflects the actual level of disruption of the energy system; (3) Recovery Index (RI) – assesses the ability of the system to mobilize resources to compensate for losses and recovery.

This approach is consistent with the logic of risk-based management, where risk is determined not only by the probability of a dangerous event occurring, but also by the scale of its consequences and the ability of the system to adapt after a crisis (Kaplan & Mikes, 2012; Boin & van Eeten, 2013).

Since the primary indicators had a significant asymmetry of distribution and contained extreme values (in particular, the number of weapons used in 2025–

2026), logarithmic transformation and normalization of variables were carried out before constructing the index:

$$X_{norm} = \frac{X_{ln} - X_{min}}{X_{max} - X_{min}},$$

where: X_{norm} – normalized value of the indicator; X_{min}, X_{max} the minimum and maximum value of the corresponding logarithmic series.

This approach ensures the comparability of heterogeneous indicators and allows integrating technical, operational and financial characteristics into a single evaluation system.

The first component of the model is the threat index, which reflects the intensity of external impact on critical infrastructure.

It includes: the number of used means of destruction; the number of massive attacks.

Since these two indicators characterize different levels of threat (the scale of an individual attack and the frequency of repeated attacks), they were combined into a composite indicator:

$$TI = \frac{Wepons_{norm} + Attacks_{norm}}{2}$$

where: $Wepons_{norm}$ – normalized number of used lesions; $Attacks_{norm}$ – normalized number of massive attacks.

The use of the arithmetic mean avoids the dominance of a single indicator and provides a balance between the intensity and regularity of threats. A similar approach is used in the formation of composite risk indicators, when individual hazard dimensions are integrated into one aggregate indicator (OECD, 2008).

The second component of the model characterizes the actual impact of imple_ mented threats on the functioning of critical infrastructure.

The duration of power supply restrictions was used as the main indicator:

$$CI = Hours_{norm}$$

where: $Hours_{norm}$– normalized number of hours of application of power consumption restrictions.

The choice of this indicator is explained by the fact that it reflects not the potential harm, but the actual result of the risk realization for society and the economy. In the context of resilience-based governance, it is the ability to maintain critical functions during a crisis that is one of the key criteria for the resilience of infrastructure systems (Bruneau *et al*., 2003).

The third component characterizes the adaptive capacity of the public administration system and its ability to ensure recovery after the implementation of threats.

The recovery index is based on the indicator of financial assistance. The formula is as follows:

$$RI = Finance_{norm}$$

where $Finance_{norm}$ is the normalized amount of financial assistance.

The inclusion of international aid in the model is explained by the modern understanding of resilience as the ability of a system not only to withstand a blow, but also to mobilize additional resources for adaptation and recovery. In complex crisis conditions, critical infrastructure often operates in a multi-level management mode, where government institutions interact with international partners, the private sector, and other support actors (Ansell *et al*., 2021).

Taking into account that a high level of threats and significant consequences reduce the resilience of the system, while a high level of recovery capabilities increases it, the integral index was formed according to the formula:

$$IICIR = RI - \frac{TI + CI}{2},$$
$$-1 \leq \text{ICKI} \leq 1.$$

The interpretation of index values is given in Table 2.

Table 2. Value levels

Meaning	Interpretation
0.50 to 1.00	High level of stability
0 to 0.49	Sufficient level of stability
-0.49 to -0.01	Reduced resistance
-1 to -0.50	critically low stability

Source: Developed by the authors

Thus, positive values mean that the compensatory and restorative mechanisms of the system outweigh the negative impact of threats, while negative values indicate a situation where the scale of risks and consequences exceeds the ability of the system to adapt.

The proposed design of the index corresponds to the concept of dynamic resilience, according to which resilience is not a static characteristic of an object, but the result of a constant interaction between threats, losses and recovery mechanisms (Holling, 1973). The results of the calculation for the period January 2023 – March 2026 are presented in Figure 6.

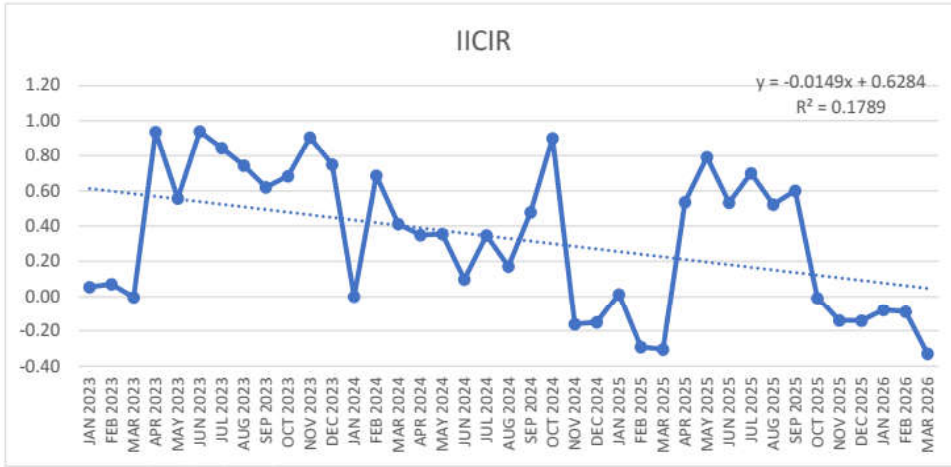

Figure 6. Dynamics of the Integral Critical Infrastructure Resilience Index of Ukraine in 2023–2026

Source: Developed by the authors

The analysis of time dynamics demonstrates a gradual change in the nature of the functioning of the energy system of Ukraine under the influence of multidimensional threats. At the initial stage (2023), the index values were mostly in the positive zone (0.56–0.94), which indicates a relatively high ability of the system to offset risks at the expense of accumulated reserves, stabilization after the winter attacks of 2022–2023, and a significant amount of international support.

During this period, there is a situation when the level of threats decreased, and recovery mechanisms remained active. That is why, even in the absence of significant attacks, the recovery index formed high values .

In 2024, there is a gradual decrease in the stability of the system. After the resumption of massive attacks in the spring of 2024, the value decreases to 0.10–0.41. This is due to the fact that the increase in the intensity of threats began to directly transform into functional losses of the power system due to the emergence of large-scale power supply restrictions.

The most critical period is observed in late 2024 - early 2025. Negative values of the index (-0.16 in November 2024; -0.31 in March 2025) indicate that the level of risk load exceeds the recovery capacity of the system. This situation corresponds to the concept of "resilience deficit", when external pressure temporarily exceeds the ability of institutions to compensate for the consequences of the crisis (Cutter *et al*., 2010).

The second crisis cycle is formed in the second half of 2025. Despite a significant increase in international support, the scale of attacks in October 2025 – February 2026 leads to the formation of negative values. The lowest values were recorded

in March 2026 (-0.33), which is due to a combination of high attack intensity, long-term power supply restrictions, and insufficient time horizon for the full restoration of damaged capacities.

At the same time, the general trend of the index demonstrates not a linear decline, but a cyclical adaptation of the system. After each wave of aggravation, there is a partial recovery of values , which indicates the presence of adaptive mechanisms of public administration and international support. Thus, the Ukrainian energy system does not demonstrate absolute resistance to threats, but the ability to function in conditions of constant crisis through a combination of protective, organizational and recovery mechanisms.

Thus, the proposed proposal allows us to move from assessing individual manifestations of the crisis to a comprehensive measurement of the effectiveness of the risk-based model of public management of critical infrastructure. Its application demonstrates that the key factor of resilience is not only the reduction of the level of threats, but the ability of institutions to quickly mobilize resources, coordinate actions and ensure the restoration of critical functions of the system.

Discussion

The results of the empirical analysis confirm and develop the key theoretical provisions of the modern literature on risk-based public management of the resilience of critical infrastructure. The proposed model, which integrates the three components of risk (Threat Index, Consequences Index and Recovery Index) into a single Integral Index of Critical Infrastructure Resilience (IICIR), demonstrates the practical applicability of the concepts of dynamic resilience (Holling, 1973; Linkov & Trump, 2019). The cyclical dynamics of IICIR, with positive values during the stages of relative stabilization and negative values during intense attacks in 2025–2026, illustrates the distinction between engineering resilience (rapid recovery) and ecological resilience (adaptive transformation of the system). Ukraine's energy infrastructure did not always return to its previous state, but retained its basic functions thanks to decentralization, international support, and institutional adaptation.

The high lag correlation between massive attacks and power supply constraints ($r = 0.952$ at lag 0) confirms the vulnerability of systems associated with the interdependence of critical infrastructure (Wells *et al*., 2022). At the same time, the increase in the effectiveness of air defense (the share of destroyed targets up to 85%) indicates the strengthening of preventive and mitigative controls within the risk management framework (Kaplan & Mikes, 2012). This is consistent with the findings of Aebi *et al*. (2024) on the role of coordination mechanisms and the 2021 legislative framework in enhancing resilience.

The reactive nature of international assistance, confirmed by a strong correlation with attack intensity ($r = 0.780$ at lag 0), is consistent with the concept of multi-level governance and robust governance in turbulent conditions (Ansell *et al*., 2021). Although external support significantly compensates for the resilience deficit (Cutter *et al*., 2010), it highlights the limited capacity of internal mechanisms to accumulate preventive reserves. This situation actualizes the recommendations of Mitoulis *et al*. (2023) on combining technical recovery with long-term peacebuilding and institutional transformations (Strahnitskyi, 2024; Zahorna & Bidiuk, 2025).

Compared to the European context (European Union, 2022; Thistlethwaite & Henstra, 2026), the Ukrainian experience demonstrates a unique "living laboratory" of resilience in the face of hybrid and kinetic threats. Spillover risks for Europe (Maznyk *et al*., 2026) and the need for stress-testing (Rimutis, 2024; Kichata *et al*., 2025) emphasize the global significance of the proposed model. Geopolitical risks and their impact on global supply chains, particularly in the energy sector, are analyzed in detail by Rasshyvalov *et al*. (2024), highlighting the need to integrate these factors into risk-based management models. IICIR fills the gap in the quantification of the full risk cycle by integrating not only technical, but also socio-economic and humanistic aspects – impact on populations, economies and social cohesion.

The results obtained have important theoretical and practical implications. Theoretically, they develop the idea of adaptive governance, demonstrating that the resilience of critical infrastructure in the face of multidimensional threats depends not so much on the reduction of the level of threats, but on the speed of resource mobilization and the ability of institutions to learn and transform. In practice, the IICIR model can serve as a monitoring tool for public administrations, allowing timely detection of resilience deficit periods and policy adjustments – from strengthening preventive protection to diversification of energy sources and development of internal reserves.

The limitations of the study are related to the use of open Energy Map data, which may contain a selection bias for "massive" attacks, as well as a focus mainly on the energy sector. Prospects for further research include extending the model to other critical infrastructure sectors, integrating social indicators (e.g., the impact of blackouts on public health and education), and benchmarking with other countries experiencing hybrid threats.

Thus, the risk-based model of public management of critical infrastructure resilience, tested on the Ukrainian experience, confirms the transition from reactive to proactive, humanistically oriented management. She emphasizes that true resilience is not only technical strength, but also the ability of the state and society to maintain human dignity, social cohesion and development prospects even in the face of a prolonged crisis.

Conclusions

The study confirms the effectiveness of the risk-based model of public management of critical infrastructure resilience in the face of multidimensional threats. The analysis of Energy Map data revealed a clear cyclical impact of military attacks on Ukraine's energy system, demonstrating a high degree of correlation between the intensity of threats, the scale of outages, and the volume of international assistance. The proposed Integral Index of Critical Infrastructure Resilience (IICIR) made it possible to comprehensively assess the dynamics of resilience, identifying periods of resilience deficit and adaptive capabilities of the system.

The results show that the resilience of critical infrastructure is determined not only by technical characteristics, but primarily by the effectiveness of institutional mechanisms, coordination of government agencies, the private sector and international partners. International assistance has played a key role in compensating for losses, but its predominantly reactive nature underscores the need to strengthen domestic preventive and cumulative mechanisms.

Theoretically, the study develops the concepts of dynamic resilience and adaptive governance, demonstrating their practical applicability in wartime. The proposed model and IICIR index can become the basis for creating a system for monitoring the resilience of critical infrastructure in Ukraine and other countries facing hybrid threats.

Promising areas for further research are the extension of the model to other infrastructure sectors, the integration of social indicators of the impact of crises on the population, as well as the development of scenarios for long-term transformation of the energy system, taking into account the principles of decentralization and green energy.

Thus, a risk-based approach to public management of critical infrastructure resilience opens up opportunities to strengthen national security, ensure the continuity of vital functions of society and preserve human potential even in the most difficult conditions of modern challenges.

References

Aebi, S., Hauri, A., & Kamberaj, J. (2024). *Critical infrastructure resilience in Ukraine: Energy, transportation, and communication*. Center for Security Studies (CSS), ETH Zürich. https://doi.org/10.3929/ethz-b-000662463

Ansell, C., Sørensen, E., & Torfing, J. (2021). The COVID-19 pandemic as a game changer for public administration and leadership? The need for robust governance responses to turbulent problems. *Public Management Review, 23*(7), 949–960. https://doi.org/10.1080/14719037.2020.1820272

Boin, A., & van Eeten, M. J. G. (2013). The Resilient Organization. *Public Management Review, 15*(3), 429–445. https://doi.org/10.1080/14719037.2013.769856

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., Shinozuka, M., Tierney, K., Wallace, W. A., & von Winterfeldt, D. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra, 19*(4), 733–752. https://doi.org/10.1193/1.1623497

Buryk, Z. (2025). Digital governance and innovative management in the public and private sectors: Strategic, social, and humanistic dimensions. Revista Administração em Diálogo, 27. https://doi.org/10.23925/2178-0080.2025v27iSI.74238

Buryk, Z., Zhuk, O., Boryshkevych, I., Piatnychuk, I., Horohotska, N., & Varenia, N. (2019). Mechanisms of management of social and economic security of the state on the basis of data formalization (case of Ukraine). In *Vision 2025: Education excellence and management of innovations through sustainable economic competitive advantage* (Proceedings of the 34th International Business Information Management Association (IBIMA) Conference, Madrid, Spain, November 13–14, 2019, pp. 11133–11135). International Business Information Management Association (IBIMA). https://ibima.org/accepted-paper/mechanisms-of-management-of-social-and-economic-security-of-the-state-on-the-basis-of-data-formalization-case-of-ukraine/

Cutter, S., Burton, C. & Emrich, C. (2010). Disaster Resilience Indicators for Benchmarking Baseline Conditions. *Journal of Homeland Security and Emergency Management, 7*(1). https://doi.org/10.2202/1547-7355.1732

DiXi Group. (2026). *Energy Map: Open data platform for the energy sector of Ukraine*. https://energy-map.info/

Energy Map. (2026a). *Information regarding massive attacks on Ukraine's critical infrastructure* [Data set]. DiXi Group. https://energy-map.info/uk/datasets/12f3148d-841a-478d-b9ed-72bf0764b286

Energy Map. (2026b). *Information regarding electricity consumption restriction measures* [Data set]. DiXi Group. https://energy-map.info/uk/datasets/0f8f9882-1fb2-47c6-81dc-31fbad914f16

Energy Map. (2026c). *Information regarding partners' assistance to the Ukrainian energy sector* [Data set]. DiXi Group. https://energy-map.info/uk/datasets/3f8e142b-33b3-49f8-949f-b244c4b28e6a

European Union. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. *Official Journal of the European Union, L 333*, 164–198. https://data.europa.eu/eli/dir/2022/2557/oj

Georgescu, A. (2025). A critical infrastructure protection perspective on the conflict in Ukraine: Recommendations for a resilient post-war Ukraine. In S. Nate (Ed.), *Ukraine's journey to recovery, reform and post-war reconstruction* (pp. 271–285). Springer. https://doi.org/10.1007/978-3-031-66434-2_19

Holling, C.S. (1973) Resilience and Stability of Ecological Systems. *Annual Review of Ecology, Evolution, and Systematics, 4*, 1-23. http://dx.doi.org/10.1146/annurev.es.04.110173.000245

Kaplan, R., & Mikes, A. (2012). Managing Risks: A New Framework. *Harvard Business Review, 90*, 48-60. https://www.scirp.org/reference/referencespapers?referenceid=3069836

Kichata, N., Tretyakov, O., Kalda, G., Pashechko, M., Doronin, Y., & Maidan, P. (2025). Implementation of a risk assessment methodology for emergency situations at

critical infrastructure objects. *Journal of Ecological Engineering, 26*(7), 286–294. https://doi.org/10.12911/22998993/203529

Linkov, I., & Trump, B. D. (2019). *The science and practice of resilience*. Springer. https://doi.org/10.1007/978-3-030-04565-4

Maznyk, L., Dvulit, Z., Wołowiec, T., Horbal, N., & Dluhopolskyi, O. (2026). Energy Resilience and Sustainability Under War: Attacks on Ukraine's Critical Infrastructure and Spillover Risks for Europe. *Sustainability, 18*(12), 6044. https://doi.org/10.3390/su18126044

Mitoulis, S.-A., Argyroudis, S., Panteli, M., Fuggini, C., Valkaniotis, S., Hynes, W., & Linkov, I. (2023). Conflict-resilience framework for critical infrastructure peacebuilding. *Sustainable Cities and Society, 91*, Article 104405. https://doi.org/10.1016/j.scs.2023.104405

OECD. (2008) *Handbook on Constructing Composite Indicators: Methodology and User Guide*. OECD Publishing, Paris. https://doi.org/10.1787/9789264043466-en

Rasshyvalov, D., Portnov, Y., Sigaieva, T., Alboshchii, O., & Rozumnyi, O. (2024). Navigating geopolitical risks: Implications for global supply chain management. *Multidisciplinary Reviews, 7*, 2024spe017. https://doi.org/10.31893/multirev.2024spe017

Rimutis, S. (2024, May 10). *Lessons of war: Ukraine's energy infrastructure damage, resilience and future opportunities*. Geopolitics and Security Studies Center (GSSC). https://www.gssc.lt/en/publication/lessons-of-war-ukraines-energy-infrastructure-damage-resilience-and-future-opportunities/

Strahnitskyi, Y. (2024). Institutional transformations in the direction of increasing the effectiveness of the state policy of critical infrastructure protection. *Public Administration and Regional Development, 23*, 28–51. https://doi.org/10.34132/pard2024.23.02

Thistlethwaite, J., & Henstra, D. (2026). Policy instruments to strengthen the cybersecurity of critical infrastructure. *Journal of Cyber Policy*, 1–21. https://doi.org/10.1080/23738871.2026.2648977

Wells, E. M., Boden, M., Tseytlin, I., & Linkov, I. (2022). Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in Disaster Science, 15*, Article 100244. https://doi.org/10.1016/j.pdisas.2022.100244

Zahorna, V., & Bidiuk, D. (2025). The impact of the destruction of Ukraine's industrial infrastructure on international cooperation and investment attractiveness. *Public Management and Policy, 10*(14). https://doi.org/10.70651/3041-2498/2025.10.11

Zayats, D., Serohina, N., Bashtannyk, O., Akimova, L., Akimov, O., & Mazalov, A. (2024). Economic aspects of public administration and local government in the context of ensuring national security. *Economic Affairs, 69*(2), 979–988. https://doi.org/10.46852/0424-2513.3.2024.23