

Risk reduction and resilience of interdependent energy and operational communication networks under hazardous impacts

Pavlo Anakhov

anakhov.pv@gmail.com

National Power Company Ukrenergo <https://orcid.org/0000-0001-9169-8560>

Viktoriia Zhebka

State University of Information and Communication Technologies <https://orcid.org/0000-0003-4051-1190>

Research Article

Keywords: cascading failures, critical infrastructure, interdependent energy and operational communication networks, risk reduction, resilience

Posted Date: September 22nd, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11093252/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.
[Read Full License](#)

Additional Declarations: The authors declare no competing interests.

Abstract

The study addresses the problem of reducing risks and enhancing the resilience of interdependent energy and operational communication networks as components of critical infrastructure exposed to natural and anthropogenic hazards, including technological, social and military impacts. Particular attention is given to intentional destructive impacts, including terrorist attacks and military actions, which may directly damage infrastructure elements or initiate cascading disruptions through interdependencies between energy and communication systems. The relevance of the study is determined by the mutual dependence of these networks: energy infrastructure requires telecommunications for monitoring, protection, control and data transmission, whereas communication infrastructure depends on a reliable power supply. Consequently, damage to one network may cause secondary failures in the other and result in cascading disruptions across interconnected infrastructure.

The study analyses scientific approaches and regulatory requirements related to critical infrastructure resilience and systematises the main internal failures, human and automated factors, and external natural and anthropogenic events that may affect the functioning of energy and operational communication infrastructure. A causal model of disruption development is proposed, in which an initial event or condition may successively lead to secondary and subsequent failures through technological, physical, information and other interdependencies between infrastructure elements. Based on this model, a system of risk reduction and resilience measures is structured, including short-term hazard forecasting and warning, long-term forecasting and risk assessment, resilient design and construction, interception and localisation of hazardous impacts, redundancy and replacement of individual systems or elements, and network reconfiguration and rerouting of energy and information flows.

The proposed approach establishes a correspondence between a hazardous event, damage factor, vulnerable infrastructure element, functional disruption and appropriate protection measure. A mathematical framework is introduced to quantify the effectiveness of individual and combined protection measures and to assess the resulting state of the protected object under a given level of external influence. This provides a methodological basis for selecting risk reduction and resilience measures for interdependent energy and operational communication networks, particularly under intentional, military and terrorist impacts and the resulting cascading propagation of disruptions.

Introduction

Military impacts on critical energy infrastructure are complex. One threat can cause several damage factors, while one damage factor can affect several interconnected infrastructure elements. Damage to one element, in turn, can cause secondary damage or disrupt the functioning of other elements due to their technological and information interdependence, resulting in the cascading propagation of damage and disruptions throughout the infrastructure [1–3]. For example, the use of missiles or unmanned weapons can cause shock effects, mechanical damage to equipment, fire, loss of power supply and disruption of information and telecommunications systems [4, 5]. The initial loss of power supply can, in

turn, lead to disruptions in telecommunications networks [2, 6], while modern critical infrastructure is simultaneously exposed to information and cyber threats [7].

Therefore, assessing the consequences of military and other intentional impacts requires consideration not only of the threat itself but also of the relationship between the threat, damage factor, vulnerable element and disruption of its functioning. This approach makes it possible to link the characteristics of a specific threat to the physical mechanism of damage, identify the most vulnerable infrastructure elements and justify the selection of appropriate protection measures. The need to account for interdependencies between energy and telecommunications networks is also confirmed by studies of the reliability and resilience of critical infrastructure [2, 8, 9].

Existing studies address individual aspects of energy infrastructure protection, including risk and vulnerability assessment, analysis of damage consequences, power system resilience, redundancy, decentralisation of generation, and restoration of damaged facilities [2, 10]. At the same time, a systematic approach that directly links a specific military or intentional threat to the relevant damage factors, vulnerable infrastructure elements and protection measures remains insufficiently developed.

The lack of such a connection complicates the informed selection of protection measures, since the same threat can produce different damage mechanisms, while the effectiveness of a particular measure depends on the nature of the impact and the properties of the vulnerable element. Studies of interdependent infrastructures show that a targeted impact on one type of infrastructure can cause cascading effects in other interconnected networks [3, 8]. Therefore, a formalised system of correspondence between threats, damage factors, vulnerable elements and protection measures is required, supplemented by a quantitative assessment of the state of the protected object.

The purpose of this study is to develop a system of correspondence between military and intentional threats to critical energy infrastructure, damage factors, vulnerable elements and appropriate protection measures, as well as a mathematical model for the quantitative assessment of the state of the protected object.

Material and method

The material of the study is the power grid and the associated information transmission network, which are exposed to wartime hazards and terrorist attacks. The objects of the study are defined as sections of the power grid and information transmission network, as well as the relevant buildings, structures, equipment, technical means and services whose functioning ensures the transmission of electricity and information.

The research method involves identifying hazards, assessing their potential impact on critical energy infrastructure facilities, identifying the corresponding damage factors, and synthesizing protection measures aimed at reducing risks and maintaining the functionality of interdependent networks.

At the first stage, a list of hazards is determined, the occurrence and propagation of which may result from processes associated with military operations and terrorist attacks. For each hazard, physical, information and other impact factors are identified that may cause damage to equipment, disrupt network functioning or reduce the availability of critical services.

At the second stage, the possible consequences of the impact of individual factors on the energy and information and telecommunications infrastructure are analysed, taking into account their interdependence and the possibility of cascading failures.

At the third stage, protection measures are synthesised to prevent hazardous events, intercept and localise hazardous impacts, reduce their consequences, reserve, replace or decommission damaged elements, and reconfigure and restore the networks.

At the fourth stage, a matrix of correspondence between damage factors and protection methods is formed, and quantitative indicators of the effectiveness of individual and combined protection measures are determined. On this basis, the residual level of hazardous impacts and the possibility of maintaining the operability of the facility under specified conditions are assessed.

Research results

Wartime and terrorist attacks on critical energy infrastructure

The scale of intentional external threats to energy infrastructure is significant. Cyberattacks constitute a distinct category of threats. According to ENISA, more than 200 cyber incidents targeting the energy sector were recorded in 2023 alone, with more than half occurring in Europe [11]. Physical attacks on energy infrastructure are also common. According to the Energy Infrastructure Attack Database, an average of about 400 attacks on energy infrastructure by non-state armed groups were recorded annually worldwide during 1980–2011 [12]. In the context of the armed aggression against Ukraine, the scale of such attacks is particularly significant: from October 2022 to September 2024, Ukraine's energy infrastructure was targeted in 1,024 Russian attacks [13]. From October 2025 to March 2026, the Russian Federation carried out at least 423 attacks on electricity generation, transmission, and distribution facilities [14]. Therefore, modern energy infrastructure should be considered subject to a combination of cyber and physical threats, including armed attacks and sabotage, which necessitates a combination of cyber defence measures, physical protection, redundancy, and network reconfiguration.

The main physical factors of explosive impact capable of disrupting the functioning of energy and operational communication networks are as follows:

1. 1. *Air blast*. Dynamic loading of buildings, supports, transformers, cable structures, and antenna masts; damage to equipment due to excessive pressure and impulse [4, 15].
2. 2. *Seismic (ground) shock*. Transmission of explosive energy through the ground, which can cause damage to foundations, underground cable lines, pipelines, substations, and other engineering structures [15, 16].
3. 3. *Fragmentation*. Penetration and damage to equipment housings, supports, insulators, cable systems, and protective structures; fragments can have a combined effect with the shock wave [5, 15].
4. 4. *Thermal radiation*. Heating and ignition of combustible materials and damage to insulation, cables, electronic components, and glazing; secondary fires may occur [15, 17].
5. 5. *Electromagnetic radiation*. Generation of electromagnetic interference, induced currents, and voltages, which can disrupt the functioning of electronic systems, communication facilities, automation, relay protection, and control systems [15, 18, 19].
6. 6. *Acoustic and infrasonic effects*. Remote propagation of explosive signals through the atmosphere, acoustic loading, and excitation of vibrations in structural elements; potential effects on sensor and monitoring systems and acoustic communication channels [15, 20].
7. 7. *Geophysical and ionospheric disturbances*. Changes in the parameters of the ionosphere, magnetic fields, and electric fields, which can deteriorate radio-wave propagation conditions and affect radio communication and radio navigation; this factor is particularly relevant to operational communication networks [21].

The probability of disruption of the functional properties of critical information infrastructure can be determined by considering four basic information security properties [22]:

$$P = 1 - \prod_{i=1}^4 (1 - q_i)$$

1

where q_1 is the probability of a breach of confidentiality, i.e. unauthorised disclosure of information; q_2 is the probability of a breach of data integrity due to their unauthorised modification, insertion, or deletion; q_3 is the probability of a breach of authenticity, i.e. unauthorised use of a resource resulting from improper identification or authentication of the subject; and q_4 is the probability of a breach of non-repudiation, i.e. the ability of a participant in an interaction to deny having performed a particular action.

Equation (1) represents the probability of at least one of the four information security properties being violated, assuming that the corresponding violation events are statistically independent.

Measures to reduce risk and ensure the stability of the power grid and the operational communication network

State of scientific research

The power grid and the operational communication network are interdependent components of critical infrastructure. The functioning of monitoring, dispatching, and data transmission systems in the power grid depends on the availability of the communication network, while the functioning of telecommunication equipment, communication nodes, and information systems requires a reliable power supply. Redundancy of power supply and communication channels can significantly reduce this dependence; however, long-term or large-scale disruptions in one of the networks can cause failures in the corresponding elements of the other network. Thus, the interdependence of the power and operational communication networks necessitates their coordinated protection, redundancy, reconfiguration, and restoration, taking into account the possibility of cascading failure propagation [2].

The interdependence of power and communication infrastructures, as well as its effect on reliability and the risk of cascading failures, has also been studied in [1].

Such interdependence becomes particularly important under natural hazards. In particular, the dependence of optical telecommunications networks on electrical networks under seismic conditions and the possibility of cascading failure propagation between these infrastructures have been studied [9].

The interdependence of energy and communication infrastructures is also particularly important under intentional external influences, including terrorist and military attacks. Such attacks can target critical elements of either the energy or communication infrastructure directly and may result in the propagation of failures between interdependent networks. Modelling of cascading failures in interdependent infrastructures during terrorist attacks has shown that accounting for physical and geographical interdependencies is essential for assessing their structural and functional vulnerability [3]. For the interdependent system comprising an electricity grid and a backbone telecommunications network, the effects of targeted attacks on nodes of one infrastructure and the associated elements of the other infrastructure have also been studied, together with the possibility of reducing the consequences of such attacks by optimising the structure of interconnections between the networks [8].

The relevance of this issue is particularly pronounced in the context of the war in Ukraine, where large-scale military attacks on critical energy infrastructure cause not only local disruptions in power supply but also systemic risks to the functioning of interconnected energy systems and related critical services [23].

Thus, existing research indicates that ensuring the resilience of power and operational communication networks should be addressed in a coordinated manner, treating them as interdependent components of a single critical infrastructure system and taking into account the possibility of mutual propagation of failures and disruptions.

Regulatory and legal support

The proposed approach is consistent with the regulatory and legal framework for the protection of critical infrastructure in Ukraine. The Law of Ukraine “On Critical Infrastructure”, dated 16 November 2021, No. 1882-IX, defines the security of critical infrastructure in terms of ensuring its functionality, continuity of operation, recoverability, integrity, and stability. The Law defines stability as the ability to function normally, adapt to changes, withstand threats, and rapidly recover from their effects. The National Plan for the Protection and Ensuring the Security and Stability of Critical Infrastructure, approved by Resolution of the Cabinet of Ministers of Ukraine No. 825-p of 19 September 2023, provides for a set of organisational and technical measures to protect critical infrastructure and ensure its stability. Certain requirements for managing security risks at Category I critical infrastructure facilities are established by Resolution of the Cabinet of Ministers of Ukraine No. 367 of 1 April 2025. The functioning of electricity infrastructure is regulated, in particular, by the Law of Ukraine “On the Electricity Market”, the Transmission System Code, and the Distribution Systems Code, while the functioning of electronic communications networks is regulated by the Law of Ukraine “On Electronic Communications”. Similar approaches are applied in the regulatory frameworks of other countries and international organisations. In the European Union, Directive (EU) 2022/2557 on the resilience of critical entities (Critical Entities Resilience, CER) establishes requirements for assessing risks and ensuring the ability of critical entities to prevent, withstand, and mitigate dangerous events and recover from their consequences while maintaining the provision of essential services. Cyber resilience in critical sectors, including energy and digital infrastructure, is further addressed by Directive (EU) 2022/2555 (NIS2).

In the electricity sector, ENTSO-E considers communication infrastructure to be an essential component of the secure operation of the interconnected European electricity system. The organisation maintains dedicated communication infrastructure for the exchange of operational data between transmission system operators (TSOs), including the Electronic Highway network for data exchange between TSOs. The cyber resilience of the electricity sector is further addressed by the Network Code on Cybersecurity, which establishes requirements for cyber risk assessment, cybersecurity, monitoring, reporting, and crisis management.

In the United States, Presidential Policy Directive 21 (PPD-21) envisages treating critical infrastructure as an integrated system, taking into account its interconnectedness and interdependencies; energy and communications systems are identified as particularly critical because of their supporting role for other sectors. In the UK, the resilience of telecommunications infrastructure is regarded as a cross-sectoral challenge, particularly because of the dependence of telecommunications networks on reliable electricity supplies. In Australia, legislation on the protection of critical infrastructure provides for mandatory risk management programmes and requirements for protecting critical assets against a range of natural, human-induced, and security threats.

Thus, international practice confirms the feasibility of comprehensive risk management and coordinated measures to ensure the resilience of interdependent energy and communication networks.

Causal relationships and cascading failures in ITS

ASCE defines hazards as natural and anthropogenic events and conditions, accidents, and intentional actions that can damage infrastructure, reduce its functionality, and impair service availability. ASCE includes energy, water, transport, and communication systems, as well as cyber, electronic, and information systems, among critical infrastructure [24].

Impacts on critical infrastructure are not necessarily independent. Several factors or events can interact sequentially, simultaneously, or in combination, resulting in a complex pattern of damage and failure propagation [24]. In such cases, the initial damage to one element can cause the failure or reduced functionality of other elements when technological, physical, information, or other dependencies exist between them.

Such interdependence is particularly important for power and operational communication networks. The power grid relies on telecommunications systems for monitoring, protection, and control, while telecommunications equipment requires a reliable power supply to operate. Consequently, the failure of one type of infrastructure can propagate to the other, resulting in a cascading failure process [2].

The cascading propagation of failures can be represented by the sequence

$$X_0 \rightarrow X_1 \rightarrow X_2 \rightarrow \dots \rightarrow X_n$$

2

,

where X_0 is the initial state or primary event, and X_i is the state of the corresponding element or subsystem after the propagation of the disruption at the i -th stage. Each subsequent state can therefore be a consequence of the preceding state while simultaneously creating conditions for a new disruption.

For interdependent power and telecommunications networks, mutual influence can also be represented as

$$E \leftrightarrow C$$

3

,

where E is the power grid and C is the operational communication network. In particular, damage to an element of the power grid can interrupt the power supply to telecommunications equipment, resulting in disruption of information transmission and dispatch control functions. The loss of control functions, in turn, can complicate the localisation of the initial failure, network switching, or restoration of power supply, thereby aggravating the initial disruption [2]. Thus, the interdependence of the networks can create conditions for the development of a cascading failure, in which the initial damage to one element propagates to other interconnected elements and subsystems.

Therefore, assessing the resilience of an ITS requires more than determining the primary damaging factor. It is also necessary to consider the possibility of its propagation between interconnected elements and the occurrence of secondary and subsequent failures. This approach makes it possible to consider the state of an ITS not as the result of a single event, but as the outcome of a sequence of interconnected events in which each subsequent failure can alter the operating conditions of other elements.

Studies of operators of critical infrastructure control centres have shown that human error, insufficient situational awareness, and excessive information load can directly affect system functioning [25].

At the same time, automation is not an unambiguously positive factor. Automation can reduce the frequency of human errors and increase the reliability of routine operations, but it can also introduce new types of system errors associated, in particular, with excessive reliance on automated decisions, loss of operator skills, and uncertainty regarding responsibility for automated actions [26]. Therefore, assessment of ITS resilience should consider both the positive effects of automation and the possibility of erroneous actions by automated systems.

Modern approaches to critical infrastructure protection also require consideration of cyber incidents, sabotage, supply chain disruptions, and other intentional or unintentional destructive influences [2].

Figure 1 presents the main factors and events that can affect the state and availability of an information and telecommunications system (ITS) in the form of a cause-and-effect diagram (Ishikawa diagram).

The factors and events that determine the state of the ITS are listed in Table 1. This classification is used as a basis for establishing the correspondence between a factor or event, the damaging factor, the vulnerable element, the resulting malfunction, and the corresponding protection measure.

Application of risk reduction and resilience measures

Taking into account the established interdependence of the power grid and the operational communication network, a scheme for applying protection measures has been developed to prevent hazardous events, reduce associated risks, and ensure the resilience of the interdependent networks. The main measures are summarised in Table 2.

A generalised scheme for applying risk reduction measures and ensuring the resilience of interdependent power and operational communication networks is shown in Fig. 2.

Matrix of correspondence of damage factors to protection methods

Determining damage factors and developing protection methods against them involves forming a matrix of correspondence between protection methods for critical energy infrastructure and wartime hazards and terrorist attacks:

$$A = \|a_{ij}\|, i = 1, 2, \dots, n, j = 1, 2, \dots, m, (4)$$

where a_{ij} is an element of the correspondence matrix that characterizes the applicability of the j -th protection method to the i -th damage factor; i is the index of the damage factor caused by shock-explosive impact or cyberattack; and j is the index of the protection method.

Examples of correspondence matrices for information transmission network protection measures and their application are given in [27, 35]. The proposed approach can be used as a basis for forming a matrix that relates wartime hazards and terrorist attacks to protection methods for critical energy infrastructure facilities.

Based on the Load and Resistance Factor Design (LRFD) principle, the limit state of the object is assessed by comparing the factored load effect with the factored resistance capacity [36–38]:

$$S = \begin{cases} 1, & \sum_{i=1}^n \gamma_i \eta_i Q_i > \varphi R, \\ 0, & \sum_{i=1}^n \gamma_i \eta_i Q_i \leq \varphi R \end{cases}$$

5

where S is an indicator of the limit state of the object: $S = 1$ indicates that the factored load effect exceeds the factored resistance capacity, whereas $S = 0$ indicates that the factored load effect does not exceed the factored resistance capacity; Q_i is the calculated value of the i -th damage factor or force effect; γ_i is the reliability factor for the corresponding load or effect; η_i is the modifying load factor that accounts for the conditions of load application and the corresponding group of limit states; R is the nominal resistance capacity of the object or its element; and ϕ is the resistance factor that accounts for uncertainty in the actual strength, failure mode, and consequences of failure.

To quantitatively account for the effectiveness of protection methods, the coefficient of the resulting protection effectiveness for the i -th damage factor is introduced:

$$K_i = 1 - \prod_{j=1}^m (1 - k_{ij})$$

6

where K_i is the resulting effectiveness of the set of applied protection methods for the i -th damage factor, and k_{ij} is the individual effectiveness of the j -th protection method for the i -th damage factor,

$$0 \leq k_{ij} \leq 1.$$

The effective value of the corresponding factor after applying protection measures is determined as

$$Q_i^* = Q_i (1 - K_i) = Q_i \prod_{j=1}^m (1 - k_{ij})$$

7

,

where Q_i^* is the effective value of the i -th damage factor after applying the protection methods.

After substituting Eq. (6), the state of the protected object is determined by substituting the effective values of the damage factors into the limit-state criterion (5):

$$S = \{1, \sum_{i=1}^n \gamma_i \eta_i Q_i \prod_{j=1}^m (1 - k_{ij}) > \varphi R, \\ \{1, \sum_{i=1}^n \gamma_i \eta_i Q_i \prod_{j=1}^m (1 - k_{ij}) \leq \varphi R$$

8

.

Here, Q_i is the initial value of the i -th damage factor, whereas Q_i^* is its effective value after applying the protection methods.

Thus, the matrix $A = ||a_{ij}||$ establishes the correspondence between damage factors and protection methods, while the coefficients k_{ij} quantitatively characterize the effectiveness of the corresponding protection methods. Eq. (6) accounts for the combined effect of multiple protection methods, and criterion (8) allows assessment of whether their combined application ensures the required state of the object under a given level of external influence.

Conclusions

1. 1. It has been established that the power grid and the operational communication network are interdependent components of critical infrastructure, whose functioning depends on the mutual availability of power supply, information exchange, monitoring, dispatching control and data transmission. Disruption of one component can cause secondary disruptions in the other and result in the cascading development of failures.
2. 2. The main natural, man-made, social and military factors and events, as well as internal failures, human actions and erroneous actions of automated systems that can disrupt the functioning of the

information and telecommunications system have been systematised. It has been shown that the nature of the consequences is determined not only by the primary impact but also by the technological, physical, information and other dependencies between the elements of interconnected networks.

3. 3. A causal model of the development of malfunctions in the information and telecommunications system has been substantiated, in which an initial event or state X_0 can sequentially cause secondary and subsequent malfunctions $X_1, X_2, \dots, X_n$. This approach makes it possible to assess the resilience of critical infrastructure by considering not only the probability of primary damage but also the possibility of its consequences propagating between interdependent elements of the energy and operational communication networks.
4. 4. A system of measures for risk reduction and resilience enhancement of interdependent networks has been developed. The system includes short-term hazard forecasting and notification, long-term risk forecasting and assessment, resilient design and construction, interception and localisation of hazardous impacts, as well as the decommissioning, replacement, duplication, dismantling and reconfiguration of individual systems or elements and the redirection of energy and information flows.
5. 5. The proposed approach establishes a correspondence between a hazardous event, damage factor, vulnerable infrastructure element, disruption of its functioning and the corresponding protection measure. This provides a methodological basis for selecting protection measures to reduce risks and enhance the resilience of the power grid and operational communication network, while accounting for the possibility of cascading effects resulting from hazardous impacts.

References

1. Korkali, M., Veneman, J., Tivnan, B. et al., Reducing cascading failure risk by increasing infrastructure network interdependence. *Sci. Rep.* 7 44499 (2017). <https://doi.org/10.1038/srep44499>
2. Liu, X., Chen, B., Chen, C. et al., Electric power grid resilience with interdependencies between power and communication networks – a review. *IET Smart Grid* 3, 182–193 (2020). <https://doi.org/10.1049/iet-stg.2019.0202>
3. Wu, B., Tang, A. & Wu, J. Modeling cascading failures in interdependent infrastructures under terrorist attacks. *Reliab. Eng. Syst. Saf.* 147, 1–8 (2016). <https://doi.org/10.1016/j.ress.2015.10.019>
4. Wu, C. & Hao, H. Modeling of simultaneous ground shock and airblast pressure on nearby structures from surface explosions. *Int. J. Impact Eng.* 31, 699–717 (2005). <https://doi.org/10.1016/j.ijimpeng.2004.03.002>
5. Grisaro, H. Y. Benamou, D., & Dancygier, A. N. Investigation of blast and fragmentation loading characteristics – field tests. *Eng. Struct.* 167, 363–375 (2018). <https://doi.org/10.1016/j.engstruct.2018.04.013>
6. *Working to stabilise mobile communications during power outages* (Ministry of Digital Transformation of Ukraine, accessed 18 September 2026), in Ukraine;

<https://thedigital.gov.ua/news/technologies/pratsyuemo-nad-stabilizatsieyu-mobilnogo-zvyazku-pid-chas-znestrumlen>

7. *CERT-UA processed nearly 6,000 cyber incidents in 2025: Hostile attack volume rose by 37%* (State Service of Special Communications and Information Protection of Ukraine, accessed 10 September 2026); <https://cip.gov.ua/en/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zroslo-na-37>
8. Rueda, D. F. & Calle, E. Using interdependency matrices to mitigate targeted attacks on interdependent networks: A case study involving a power grid and backbone telecommunications networks. *Int. J. Crit. Infrastruct. Prot.* 16, 3–12 (2017). <https://doi.org/10.1016/j.ijcip.2016.11.004>.
9. Jiménez, D., Gacitúa, L., Cancela, H. et al. Reliability assessment of critical infrastructure under seismic hazard: Dependence of telecommunication network on electricity grid. *IEEE Access* 14, 72085–72102 (2026). <https://doi.org/10.1109/ACCESS.2026.3689367>.
10. Shi, Q., Li, F., Olama, M. et al. Winstead, Network reconfiguration and distributed energy resource scheduling for improved distribution system resilience. *Int. J. Electr. Power Energy Syst.* 124, 106355 (2021). <https://doi.org/10.1016/j.ijepes.2020.106355>.
11. *Ukraine's energy security and the coming winter* (International Energy Agency, accessed 18 September 2026); <https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter>
12. Giroux, J., Burgherr, P., & Melkunaite, L. Research note on the Energy Infrastructure Attack Database (EIAD). *Perspect. Terror.* 7, 113–125 (2013). <https://www.jstor.org/stable/26297069>.
13. *In two years, Russia has attacked Ukraine's energy sector more than 1,000 times: German Galushchenko* (Cabinet of Ministers of Ukraine, accessed 18 September 2026); <https://www.kmu.gov.ua/en/news/za-dva-roky-rosiia-atakuvala-ukrainsku-enerhetyku-ponad-1000-raziv-herman-halushchenko>
14. *Attacks against Ukraine's energy infrastructure and update on the human rights situation in Ukraine, 1 December 2025–31 May 2026* (Office of the United Nations High Commissioner for Human Rights, accessed 10 September 2026). <https://ukraine.ohchr.org/en/Attacks-against-Ukraine-s-energy-infrastructure-and-update-on-the-human-rights-situation-in-Ukraine-1-December-2025-31-May-2026>
15. Chernogor, L. F. Geophysical effects and geoecological consequences of mass chemical explosions at military warehouses in Artemovsk. *Geofizicheskii Zhurnal* 26, 31–44 (2004) (in Russian).
16. Westine, P. S. Ground shock from the detonation of buried explosives. *J. Terramech.* 15, 69–79 (1978). [https://doi.org/10.1016/0022-4898\(78\)90025-3](https://doi.org/10.1016/0022-4898(78)90025-3).
17. Zhang, Y. & Zhang, Q. Temperature response and damage mechanism of glass under thermal radiation of strong explosion. *Int. J. Heat Mass Transf.* 228, 125716 (2024). <https://doi.org/10.1016/j.ijheatmasstransfer.2024.125716>.
18. Kolsky, H. Electromagnetic waves emitted on detonation of explosives. *Nature* 173, 77 (1954). <https://doi.org/10.1038/173077a0>.
19. Ren, H., Chu, Z. & Li, J. Study on electromagnetic radiation generated during detonation. *Propellants Explos. Pyrotech.* 44, 1541–1553 (2019). <https://doi.org/10.1002/prop.201900118>.

20. Chernogor, L. F. & Garmash, K. P. Magnetospheric and ionospheric effects accompanying the strongest technogenic catastrophe. *Geomagn. Aeron.* 58, 673–685 (2018).
<https://doi.org/10.1134/S0016793218050031>.
21. Kuzminykh, I., Carlsson, A., Yevdokymenko, M. et al. Investigation of the IoT device lifetime with secure data transmission. In: O. Galinina, S. Andreev, S. Balandin, Y. Koucheryavy (Eds.), *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, Springer, Cham, pp. 16–27 (2019). https://doi.org/10.1007/978-3-030-30859-9_2
22. Popenhagen, S. K., Bowman, D. C., Zeiler, C. et al. Acoustic waves from a distant explosion recorded on a continuously ascending balloon in the middle stratosphere. *Geophys. Res. Lett.* 50, e2023GL104031 (2023). <https://doi.org/10.1029/2023GL104031>.
23. Maznyk, L., Dvulit, Z., Wołowiec, T. et al. O. Dluhopolskyi, Energy resilience and sustainability under war: Attacks on Ukraine's critical infrastructure and spillover risks for Europe. *Sustainability* 18, 6044 (2026). <https://doi.org/10.3390/su18126044>.
24. *Policy statement 518: Unified definitions for critical infrastructure resilience* (American Society of Civil Engineers, accessed 10 September 2026). <https://www.asce.org/advocacy/policy-statements/ps518---unified-definitions-for-critical-infrastructure-resilience/>
25. Ofte, H. J. The awareness of operators: A goal-directed task analysis in SOCs for critical infrastructure. *Int. J. Inf. Secur.* 23, 3253–3282 (2024). <https://doi.org/10.1007/s10207-024-00872-6>.
26. Pöhler, J., Flegel, N., Mentler, T. et al. Keeping the human in the loop: Are autonomous decisions inevitable? *i-com* 24, 9–25 (2025). <https://doi.org/10.1515/icom-2024-0068>.
27. Mukhin, V. Anakhov, P., Zhebka, V. et al. Protecting hybrid information transmission network from natural and anthropogenic hazards. *Int. J. Comput. Netw. Inf. Secur.* 14, 1–10 (2022).
<https://doi.org/10.5815/ijcnis.2022.05.01>.
28. *Early Warnings for All in Focus: Hazard Monitoring and Forecasting* (World Meteorological Organization, accessed 18 September 2026); <https://wmo.int/files/early-warnings-all-focus-hazard-monitoring-and-forecasting-2025>
29. *A pre-winter assessment* (International Energy Agency, accessed 10 September 2026).
<https://www.iea.org/reports/ukraines-energy-security/a-pre-winter-assessment>
30. *DREAM public investment program* (Cabinet of Ministers of Ukraine, accessed 10 September 2026);
<https://dream.gov.ua/public-program/DREAM-UA-060825-7846A759?fromUri=%2Fsectoral-portfolio%2F1100>
31. *As Ukraine heads into another heating season, six measures can help improve energy security* (International Energy Agency, accessed 18 September 2026); <https://www.iea.org/reports/ukraines-energy-security/as-ukraine-heads-into-another-heating-season-six-measures-can-help-improve-energy-security>
32. McCarthy, J. J., Faatz, D., Perper, H. et al. *Identity and access management for electric utilities* (NIST Special Publication 1800-2, accessed 10 September 2026);

<https://csrc.nist.gov/pubs/sp/1800/2/final>

33. *How to stay connected during power outages* (Ministry of Digital Transformation of Ukraine, accessed 18 September 2026), in Ukraine; <https://thedigital.gov.ua/news/how-tos/iak-zalyshatysia-na-zviazku-pid-chas-znestrumlen>.
34. Anakhov, P., Zhebka, V., Popereshnyak, S. et al. Protecting objects of critical information infrastructure from wartime cyber attacks by decentralizing the telecommunications network. *CEUR Workshop Proc.* 3550, 240–245 (2023). <https://ceur-ws.org/Vol-3550/short7.pdf>.
35. Anakhov, P., Zhebka, V., Berkman, L. et al. Increasing functional stability of telecommunications network in the depressed zone of HPS reservoir. In: M. Klymash, A. Luntovskyy, M. Beshley, I. Melnyk, A. Schill (Eds.), *Emerging Networking in the Digital Transformation Age*, Springer, Cham, pp. 214–230 (2023). https://doi.org/10.1007/978-3-031-24963-1_12.
36. Kumar, P. & Samui, P. Reliability-based load and resistance factor design of an energy pile with CPT data using machine learning techniques. *Arab. J. Sci. Eng.* 49, 4831–4860 (2024). <https://doi.org/10.1007/s13369-023-08253-2>.
37. Song, J., Shen, J.-D. J., Huang, C. et al. Analysis of LRFD factors for a linear limit-state equation with correlated and time-independent random variables: Closed-form formulation and numerical algorithm. *Eng. Struct.* 286, 116049 (2023). <https://doi.org/10.1016/j.engstruct.2023.116049>.
38. Wang, J., Ye, X., Zheng, W. et al. Improved calculation of load and resistance factors based on third-moment method. *Appl. Sci.* 11, 9107 (2021). <https://doi.org/10.3390/app11199107>.

Figures

Figures are available in the Supplementary Files section.

Table 2

Table 2 is available in the Supplementary Files section.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- [ExtendedData.docx](#)