POLITYKA ENERGETYCZNA – ENERGY POLICY JOURNAL

2026 ✦ Volume 29 ✦ Issue 2 ✦ 135–164

DOI: 10.33223/epj/213910

Oleh Semenenko[1], Svitlana Zakharova[2], Andrii Gorlichenko[3], Oleksandr Signaievskyi[4], Oleksandr Fedchenko[5]

Innovative technologies for protecting Ukraine's critical energy infrastructure under wartime conditions

Abstract: This study was aimed at a comprehensive analysis of protection technologies for energy facilities of critical infrastructure in Ukraine under wartime conditions. The study used a mixed-method approach combining literature review, comparative analysis, and evaluation of national and international data to assess protection technologies for critical energy infrastructure under wartime conditions. As a result of the study, it was noted that in 2021, Ukraine's energy infrastructure had a capacity of 53.3 GW and produced 158.4 billion kWh, but after the Russian invasion in 2022, it lost two-thirds of its capacity – by mid-2024, it totaled ~15.4 GW due to the occupation of the Zaporizhzhia Nuclear Power Plant and the destruction of key facilities. It was established that

✉ Corresponding Author: Oleh Semenenko; e-mail: olehsemenenko4@gmail.com

[1] Central Research Institute of the Armed Forces of Ukraine, Ukraine; ORCID iD: 0000-0001-6477-3414; e-mail: olehsemenenko4@gmail.com

[2] Department of Provision of Fuels and Lubricants, Odesa Military Academy, Ukraine; ORCID iD: 0009-0000-0366-912X; e-mail: s_zakharova@outlook.com

[3] Department of Foreign Languages, Odesa Military Academy, Ukraine; ORCID iD: 0009-0005-9505-3272; e-mail: gorlichenko.a09@hotmail.com

[4] Department of Civil and Industrial Safety, National Aviation University, Ukraine; ORCID iD: 0000-0001-7027-6887; e-mail: signaievskyi@outlook.com

[5] Research Department of International Scientific Cooperation, Central Research Institute of the Armed Forces of Ukraine, Ukraine; ORCID iD: 0000-0002-2514-978X; e-mail: o.fedchenko@hotmail.com

© 2026. The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution-ShareAlike International License (CC BY-SA 4.0, http://creativecommons.org/licenses/by-sa/4.0/), which permits use, distribution, and reproduction in any medium, provided that the Article is properly cited.

modern technologies and means of protection of energy facilities played an important role in ensuring the resilience of the energy system to physical and cyber threats, especially in the context of hybrid warfare. It was also noted that cybersecurity, reinforced by monitoring systems integrated with artificial intelligence, as well as technologies for data protection and network segmentation, significantly improved the security of digital control systems, allowing resistance to sophisticated cyberattacks. Modern technologies, particularly 3D printing, allowed for the rapid production of spare parts for equipment, while modular transformers, compact and easy to transport, ensured the quick restoration of energy supply. The results of the study could be used to develop and implement comprehensive protection systems for energy facilities in Ukraine's frontline regions, taking into account the real conditions of combat and limited resources.

Keywords: hybrid threats, unmanned aerial vehicles, rapid recovery, international standards, cyberattacks, physical barriers

Introduction

The protection of energy facilities of critical infrastructure, such as power plants, substations, and power transmission lines, was strategically important for ensuring national security, economic stability, and the uninterrupted functioning of society – particularly in Ukraine, where, since 2022, the war had continued, accompanied by attacks on the energy system. The vulnerability of centralized energy networks, where damage to a key facility could cause large-scale power outages, threatened civilian life, industry, medical, and defense structures, highlighting the need for a comprehensive approach to protection that encompassed both physical and digital aspects.

The study of modern technologies and defense strategies, adapted to the conditions of hybrid conflict, as well as the analysis of international experience of leading countries, was critically important for developing effective solutions that would enable Ukraine to preserve energy supply and meet European security standards. In the global context of increasing complex threats, such studies had universal significance, contributing to the creation of resilient energy systems capable of withstanding contemporary challenges and ensuring societal stability.

It should be noted that the protection of energy facilities of critical infrastructure was a multifaceted issue requiring the integration of physical, cyber, and organizational measures – especially in the context of war in Ukraine, where physical and cyberattacks on the energy system had become systematic.

In the work of Koval et al. (2022), organizational and technical principles of building an engineering protection system for energy facilities were studied, and a model of second-level fortifications for substations was proposed to increase resistance to physical attacks; however, insufficient attention was paid to the integration of these solutions with modern digital control systems, limiting the effectiveness under hybrid threats.

In the study by Liubovetskyi et al. (2025), emphasis was placed on ensuring the functioning of critical infrastructure in the context of modern warfare, particularly through the decentralization

of energy systems and the use of modular transformers for rapid recovery; however, the work did not detail practical mechanisms for scaling these solutions in frontline regions, reducing its applied value.

In the work of Manuilov (2023), the provision of cybersecurity for critical infrastructure in the context of cyber warfare was analyzed, and the importance of monitoring systems for protecting various systems from attacks was emphasized, but without sufficiently analyzing the interaction between cyber protection and physical measures, which was critical for the comprehensive protection of energy facilities.

As a result of the work by Volkov et al. (2023), the protection of critical infrastructure facilities from airstrikes was studied by combining various forces and means, and a model for integrating tools to improve the protection of substations and power plants from missile attacks and drones was proposed; however, the economic feasibility of the proposed solutions was not sufficiently analyzed, which complicated the large-scale implementation under limited funding.

In the study by Lehto (2022), cyberattacks on critical infrastructure were analyzed, focusing on the vulnerabilities of control systems; however, the work was limited to theoretical analysis and did not offer specific practical recommendations for countries at war, such as Ukraine. In the work by Plėta et al. (2020), cyberattacks on energy infrastructure were examined, and case studies of attacks on electricity networks were presented, emphasizing the role of network segmentation and international cooperation in enhancing cyber resilience; however, it did not fully correspond to the context of the analysis, failing to account for modern hybrid threats such as combined physical and cyberattacks, characteristic of the war in Ukraine.

As a result of the work by Kootala et al. (2023), the threats posed by drones to energy critical infrastructure were investigated, with a focus on unmanned aerial vehicle (UAV) attacks, and the use of anti-drone systems to neutralize threats was proposed; however, the economic efficiency of such solutions was not analyzed, which complicated the widespread implementation under constrained financial conditions.

In the study by Di Pietro et al. (2021), new dimensions of information warfare were analyzed, in particular, the impact of cyberattacks on critical infrastructure, emphasizing the importance of monitoring systems to protect critical infrastructure systems; however, the work lacked specific examples of adapting these approaches to the context of real military conflict, reducing its practical value for Ukraine.

In the study by Zhang and Kusrini (2021), an autonomous long-range drone detection system for the protection of critical infrastructure was presented, with emphasis on its ability to operate in harsh weather conditions; however, the lack of analysis of the integration of this system with other defense means, such as electronic security or air defense, limited its effectiveness in the comprehensive protection of energy facilities.

The aim of this work was to conduct a comprehensive analysis of the approach to the protection of energy facilities of critical infrastructure in Ukraine under wartime conditions by studying modern technologies and means of protection, evaluating practical experience, and international standards. To achieve this goal, several key tasks were defined, including:

- analyzing modern protection technologies, including anti-drone systems, cyber protection using artificial intelligence, decentralized energy hubs, and innovative solutions under hybrid threats;
- assessing Ukraine's practical experience against international practices of countries such as the USA, Israel, and countries of the EU to adapt advanced approaches;
- identifying key implementation challenges and developing practical recommendations to overcome them, contributing to the rapid recovery and long-term resilience of energy infrastructure.

1. Materials and methods

A thorough methodology that integrated both qualitative and quantitative techniques was used to perform the study. Qualitative methods included a systematic literature review, analysis of case studies on attacks and recovery of energy facilities, and expert interviews with energy operators and cybersecurity specialists. Quantitative methods included gathering and statistically analyzing information from national and international reports on installed capacity, infrastructure losses, energy generation, and the efficacy of protection measures. These techniques were supported by an evaluation of operational difficulties, a comparison with global norms, and the creation of useful suggestions for enhancing the resilience of Ukraine's vital energy infrastructure.

The basis of the study was the collection of data from both secondary and primary sources. Scientific literature, particularly analytical reports from think tanks such as the Pacific Northwest National Laboratory (2025), was used to analyze modern technologies and practices, enabling the assessment of the capabilities of artificial intelligence, 3D printing, and other technologies.

The regulatory framework included the Decision of the National Security and Defense Council of Ukraine "On the Organization of Protection and Ensuring the Security of the Functioning of Critical Infrastructure and Energy Facilities of Ukraine in the Context of Military Operations" (2023), Resolution of the Cabinet of Ministers of Ukraine No. 518 "On Approval of the General Requirements for Cyber Defence of Critical Infrastructure Facilities" (2019), as well as international standards ISO/IEC No. 27001:2022 "Information Security Management Systems" (2022), the National Institute of Standards and Technology (2025), and the NIS2 Directive "Securing Network and Information Systems" (2023), which helped to analyze regulatory approaches.

Reports from international organizations, such as the U.S. Agency for International Development (2025), the European Union Agency for Cybersecurity (2025), and the Cybersecurity and Infrastructure Security Agency (2021) report, provided information on cyber threats, physical attacks, and global protection practices. Industry sources, including publications from the Centre for European Policy Analysis, "Ukraine Teaches Europe Cyber Lessons" (Ilves,

2025) and Eurelectric, “Cybersecurity in the Power Sector” (2025), highlighted real attack cases and technological solutions.

Primary data included information from the National Energy Company (NEC) “Ukrenergo” (2025), as well as an analysis of specific cases, such as response measures to the 2022–2023 attacks, gathered from open sources, including reports from the United Nations (2024), reports by the United Nations Development Programme (2023) on the assessment of the state of Ukraine’s energy infrastructure, and publications from Defence Express (Drone Hunters are… 2023).

The study used data on Ukraine’s energy infrastructure from 2021 to mid-2024. The year 2021 was chosen as the baseline to reflect the state of electricity generation prior to full-scale war and installed capacity, while data from 2022 to mid-2024 capture the impacts of the Russian invasion, including physical destruction, occupation of facilities, and cyberattacks. The reports by NEC “Ukrenergo” (2025) and the Ministry of Energy of Ukraine (2025) were analyzed. This period allows for a comprehensive assessment of infrastructure losses, the effectiveness of protection measures, and the adaptation of recovery strategies under wartime conditions.

To analyze the key approaches, technologies, and standards for protecting critical energy infrastructure from hybrid threats in the EU (Germany, the Baltic States), the USA, and Israel, a comparative study of official documents, reports, and strategies was conducted, including the NIS2 Directive “Securing Network and Information Systems” (2023), European Union Agency for Cybersecurity (2025) standards, National Institute of Standards and Technology (2020), and Israel’s critical infrastructure protection policy (International Trade Administration 2025; The U.S.-Israel… 2021; Tabansky 2025). The analysis focused on chosen countries as they exemplify advanced energy protection and cybersecurity practices. They offer lessons on decentralization, AI-based danger prediction, and active defense that might be applied to Ukraine’s wartime situation.

To assess challenges and develop recommendations, a detailed analysis was conducted, which helped to identify both advantages and key challenges. Quantitative analysis included an evaluation of data on energy infrastructure losses, the effectiveness of technologies, and the volume of international assistance. Qualitative analysis focused on interpreting case studies and evaluating regulatory documents.

Data synthesis was carried out by categorizing by protection aspect (including active defense, passive protection, cyber defense, physical protection, rapid recovery systems, personnel training and coordination, and regulatory compliance), which allowed for the development of recommendations for improving the protection of critical energy infrastructure. This methodology ensured a structured approach to analysis, taking into account wartime constraints such as security risks and logistical difficulties. The combination of secondary and primary sources, as well as comparative analysis, allowed for comprehensive conclusions that reflected both the current state of protection of Ukraine’s critical energy infrastructure and the prospects for its improvement under hybrid threat conditions.

The analysis’s worldwide reports may be biased by geopolitical interests, institutional funding, and methodological constraints because they reflect the organizations’ opinions and priorities. U.S. or EU agencies may prioritize solutions that match their policies or technology

choices, which may not apply to Ukraine's wartime circumstances. The authors corrected these biases by critically evaluating the reports within the conflict's unique problems and settings, taking local realities and practical restrictions into consideration when drawing findings.

2. Results

2.1. Impact of hybrid warfare on Ukraine's energy infrastructure

Energy facilities form the foundation of modern society and the economy. The energy facilities ensure the uninterrupted supply of electricity, heat, fuel, and other resources necessary for the operation of industry, transport, healthcare institutions, and the daily needs of the population (Stoliarov, 2024). However, in the context of military actions – especially in modern hybrid warfare – these facilities become priority targets for attacks.

Missile strikes, drone attacks, cyberattacks, and sabotage operations are aimed at destroying or disabling energy infrastructure, which can lead to humanitarian crises, economic collapse, and the weakening of a country's defense capabilities. In Ukraine, since 2022, Russian attacks on energy infrastructure have caused catastrophic consequences: by mid-2024, the country had lost approximately two-thirds of its electricity generation capacity before the full-scale war, which has become one of the greatest challenges for the state during wartime (Fig. 1).

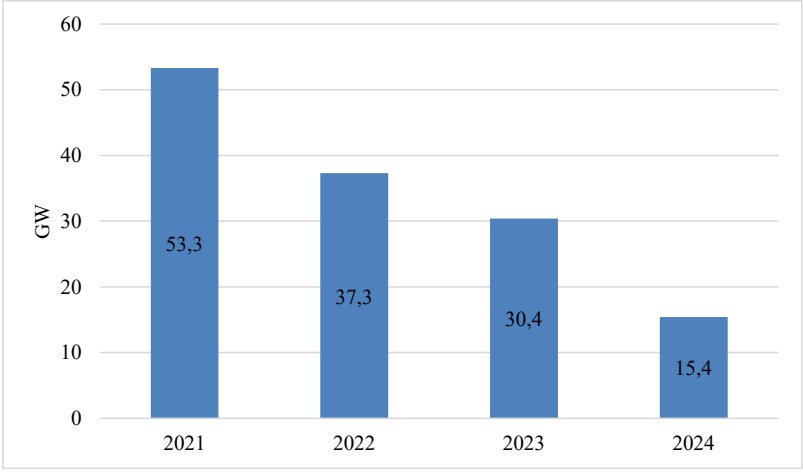

Fig. 1. Dynamics of Ukraine's electricity generation capacity in 2021–2024
Source: developed by the authors based on NEC "Ukrenergo" (2025), United Nations (2024), United Nations Development Programme (2023), Defense Express (2023), Ministry of Energy of Ukraine (2025)

Rys. 1. Zmiany mocy wytwórczych energii elektrycznej w Ukrainie w latach 2021–2024

In 2021, Ukraine's installed electricity generation capacity amounted to 53.3 GW, and electricity production reached 158.4 billion kWh. The main sources were nuclear power (54.4%), thermal power plants (23.5%), hydroelectric power stations (8.64%), combined heat and power (6.4%), and renewable sources (2.2%). Since the beginning of Russia's full-scale invasion in 2022, the energy system has suffered significant losses. In 2022, electricity production fell to 148.8 billion kWh, and generation dropped by 30% due to the occupation of the Zaporizhzhia Nuclear Power Plant (6 GW) and damage to other facilities. In 2023, electricity production decreased by 19.4% compared to 2022, amounting to 36.5 billion kWh from January to April.

Nuclear generation declined by 44%, hydropower by 29%, and renewables by 24%. By mid-2024, Ukraine had lost around two-thirds of its generation capacity before full-scale war (total losses ~22.6 GW). Notably, 100% of Centrenergo's capacity (Trypilska, Zmiivska, and Vuhlehirska Thermal Power Plants), 80% of combined heat and power plants, and two hydroelectric power plants were destroyed, and the Zaporizhzhia Nuclear Power Plant remained under occupation. Approximately 15.4 GW remained, a significant portion of which were solar power plants, which are less efficient in winter. Thus, from 53.3 GW in 2021, by mid-2024, capacity had fallen to around 15.4 GW, representing less than one-third of the level prior to full-scale war.

The first and most obvious threat to the security of energy facilities is physical attacks (United Nations, 2024; United Nations Development Programme, 2023). Precision missile strikes, artillery shelling, and UAV attacks can destroy key elements of the energy system, such as transformers, generators, or transmission lines. For example, massive missile attacks on Ukrainian substations in 2022–2023 led to power outages for millions of people, especially during winter, when energy demand increases.

Kamikaze drones, such as the Shahed-136, have become particularly dangerous due to their low cost, quantity, and ability to strike targets at long distances. Such attacks not only destroy equipment but also complicate rapid repairs due to a shortage of spare parts and logistical issues. The second serious challenge is cyberattacks aimed at disrupting the operation of automated control systems, particularly Supervisory Control and Data Acquisition (SCADA) systems.

These systems are responsible for real-time monitoring and control of energy facilities, and the failure can cause chaotic disruptions in energy supply. In current conditions, cyberattacks are becoming increasingly sophisticated, using artificial intelligence and social engineering techniques to infiltrate the networks of critical infrastructure operators. Social engineering methods, including phishing, pretexting, baiting, and impersonation, manipulate people into disclosing confidential information or compromising security. These attacks can also be synchronized with physical strikes, creating a combined threat.

Terrorist threats and acts of sabotage also pose a significant risk. In wartime, sabotage groups may attempt to blow up equipment, damage gas pipelines, or disable control systems (Knapik 2017). Such actions are difficult to anticipate because of being often carried out by small groups using improvised tools or explosives. Moreover, sabotage may be aimed not only at physical destruction, but also at spreading panic among the population or discrediting authorities by disrupting energy supplies.

Cascading effects caused by the interdependence of energy system components exacerbate the situation, as the energy infrastructure functions as a complex network where damage to one facility can trigger a chain reaction. For example, the failure of a key substation can lead to overloads in other parts of the network, resulting in widespread blackouts. These effects complicate recovery efforts, since repairing one facility requires stable operation of other system components.

In Ukraine, cascading outages became a notable issue during mass attacks on the energy system between 2022 and 2024, when damage to several critical facilities caused prolonged blackouts across entire regions (United Nations 2024). Limited resources also significantly complicate the protection and recovery of energy facilities, as access to materials, equipment, and qualified specialists is often restricted during wartime.

Supply chains are disrupted by hostilities, and funding for the protection of critical infrastructure competes with other military needs. Rapid restoration of damaged facilities requires resources and coordination between state agencies, private energy operators, and international partners.

2.2. Passive protection strategies for Ukraine's critical energy infrastructure

Passive protection of critical energy infrastructure is one of the key strategies for ensuring its security in combat conditions (United Nations Development Programme 2023). It involves the use of engineering and structural solutions aimed at minimizing damage from aerial, ground, or sabotage attacks without employing active countermeasures such as air defense systems or electronic warfare.

The main goal of passive protection is to create physical barriers capable of withstanding or reducing the impact of blast waves, shrapnel, drone strikes, or other threats, preserving the functionality of critical equipment. In Ukraine, passive protection has become an integral part of the energy system's resilience strategy. The main means of passive protection actively used to safeguard energy facilities are discussed below.

Concrete protective structures are among the most common and reliable means of passive protection. Since March 2023, large-scale construction of second-level concrete fortifications began in Ukraine for key energy facilities, including 22 substations and 63 autotransformers across 14 regions (United Nations Development Programme 2023; Drone Hunters are… 2023; Ministry of Energy of Ukraine 2025).

These structures are designed to protect against missile shrapnel, blast waves, and partial direct impacts. Concrete constructions and fortifications usually consist of massive walls or full-scale bunkers surrounding critical equipment (Babak et al. 2021). The constructions can withstand significant loads, allowing substations to remain operational even after massive missile strikes. In some cases, concrete structures are reinforced with sand or earth embankments to further absorb blast energy and reduce the risk of damage.

Modular shelters are another innovative passive protection solution (Pshemyska 2024; Pyshkin 2024; Ismanzhanov and Tashiev 2016). These quick-to-install structures are designed to protect individual equipment components from kamikaze drones and missile shrapnel. Modular shelters are made from high-strength materials such as steel, composite panels, or reinforced concrete and can be installed within days, which is critical in wartime (Kubiczek et al. 2023; Marignetti et al. 2023).

The advantage lies in the mobility and adaptability: the shelters can be quickly dismantled, relocated, or modified as needed. In Ukraine, such shelters are actively used to protect high-voltage transformers – some of the most expensive and vulnerable components of the energy system (Skochko et al. 2024). Following attacks on substations in 2022–2023, where transformer damage caused prolonged power outages, modular shelters began to be installed as a temporary measure until permanent concrete structures could be completed.

Anti-drone nets and barriers play an important role in defending against small UAV carrying explosives, such as First Person View (FPV) drones or commercial quadcopters repurposed for attacks. These nets, made from high-strength synthetic materials or metal alloys, are installed over critical areas of energy facilities, such as transformer yards or fuel depots. The nets can stop drones or trigger premature detonation of explosives, significantly reducing the risk of equipment damage.

In Ukraine, anti-drone nets became widely used following a rise in kamikaze drone attacks, which posed a serious threat to energy infrastructure. These barriers are a cost-effective solution as the installation requires relatively low capital investment, yet the effectiveness against cheap UAVs is high. In some cases, nets are reinforced with metal plates or other protective elements to improve resistance to shrapnel.

Passive protection also includes additional engineering solutions such as protective screens, blast-resistant window films in control rooms, and reinforced equipment foundations (United Nations Development Programme 2023). For example, blast-resistant films can prevent glass from shattering in control buildings, protecting personnel and monitoring systems from harm.

Foundation reinforcement allows equipment to withstand vibrations from explosions, which is particularly important for sensitive components such as turbines or high-voltage circuit breakers (Ismanzhanov et al. 2012). Although less large-scale than concrete structures, these measures play an important role in the comprehensive protection of facilities. The implementation of passive protection measures in Ukraine has yielded results through the construction of second-level fortifications, but faces several challenges. First, the construction of concrete fortifications and modular shelters requires substantial financial and material resources, which are limited during wartime. Second, the speed of deploying such measures often lags behind the pace of attacks, necessitating optimization of logistics and construction processes. Third, coordination between state authorities, private energy operators, and international partners is needed to ensure timely funding and supply of materials. Despite these difficulties, passive protection remains a critically important element of the energy facility protection strategy, ensuring resilience to physical threats and supporting rapid recovery after attacks.

2.3. Active protection measures for Ukraine's critical energy infrastructure

Active protection of critical energy infrastructure, in turn, involves the use of technologies and systems capable of detecting, neutralizing, or destroying threats in real time, such as missile strikes, UAV attacks, or sabotage. Unlike passive protection, which focuses on fortifying facilities, active protection aims to prevent enemy assets from striking the targets or to neutralize them before impact. In modern military conflicts – particularly the Russia-Ukraine war – active protection plays a key role in ensuring the security of energy facilities.

In Ukraine, where energy infrastructure has faced systematic attacks since 2022, air defense systems, interceptor drones, and electronic warfare tools are actively used. These technologies effectively counter both precision missiles and low-cost kamikaze drones, protecting critical facilities and minimizing the risk of power outages. Table 1 provides a detailed analysis of case responses to attacks on Ukraine's critical infrastructure.

Air defense systems formed the basis of the active protection of energy-related critical infrastructure from aerial threats. Localized air defenses, such as surface-to-air missile systems or mobile fire teams, were deployed to protect key sites from missile strikes and UAV attacks. In Ukraine, the Armed Forces of Ukraine and the National Guard actively used such systems to shield energy infrastructure. For example, anti-aircraft complexes such as the S-300, Patriot, or NASAMS were capable of intercepting ballistic and cruise missiles, which posed a serious threat to large power plants and substations. To counter drones, mobile fire teams equipped with man-portable air defense systems, such as "Igla" or "Stinger", as well as machine guns and cannons, were widely used. In addition, local air defenses were complemented by early warning systems, such as radar, which provided timely responses to threats.

Interceptor drones represented an innovative solution for countering hostile UAVs, especially low-cost kamikaze drones widely used to attack energy infrastructure (United Nations 2024; United Nations Development Programme 2023; Drone Hunters are… 2023). These specialized drones were equipped with capture systems (e.g., nets) or destruction mechanisms (laser or kinetic devices) and were capable of responding swiftly to threats within a limited radius.

In Ukraine, interceptor drones began to be actively developed and used from 2023, when a sharp increase in drone attacks necessitated cost-effective solutions. Such drones could autonomously detect targets using thermal imagers or radar and neutralize targets through direct collision or by dropping small explosive devices. For example, Ukrainian designs featuring integrated nets or electromagnetic pulses demonstrated high effectiveness against commercial quadcopters repurposed for attacks. The advantage of interceptor drones lies in the mobility, lower cost compared to traditional air defense systems, and the ability to operate in environments where the deployment of large missile systems was impractical. The drones were particularly useful for defending against low-flying drones that were difficult to detect using conventional radar.

Table 1. Analysis of cases of response to attacks on critical infrastructure facilities in Ukraine

Tabela 1. Analiza przypadków reagowania na ataki na obiekty infrastruktury krytycznej na Ukrainie

Case	Date and place	Attack description	Consequences	Response measures	Effectiveness of measures
Massive attack on Ukraine's energy system, October–November 2022	October–November 2022, all of Ukraine (including Kyiv, Kharkiv, Dnipro)	A series of attacks using 84 cruise missiles and 24 kamikaze drones targeting power plants, substations, and power lines	Loss of about 50% of the power grid, large-scale blackouts	Deployment of local air defense systems to intercept missiles and drones (21 out of 23 missiles shot down on April 28, 2023). Power engineers of NEC "Ukrenergo" carried out emergency repairs, restoring up to 30% of damaged capacities by the end of 2022	Partial restoration of power supply by the beginning of winter 2022, but full restoration was complicated by repeated attacks
Attack on Uman energy infrastructure	October 22, 2022, Uman, Cherkasy region	Damage to energy infrastructure facilities that provide electricity to Uman and surrounding areas	Almost a day without electricity in the city, power outages in critical infrastructure (water supply, hospitals)	Strengthening air defense in the region to protect against drones. Planning to integrate solar panels with diesel generators to increase autonomy	Power was restored quickly, but reliance on generators increased costs
Attack on substation in Kyiv region	November 15, 2022, Kyiv region	Russian Shahed-136 drones and missiles attacked a key substation that provides electricity to part of the Kyiv region, attempting to disable it	Temporary power outage for 150,000 households, disruption of local water and heating services	Use of the Bukovel-AD electronic warfare system to jam drone signals at a distance of up to 20 km, which allowed to neutralize 3 out of 5 drones; local air defense intercepted 2 missiles. Second-level concrete reinforcements around the substation reduced damage from debris	Active and passive protection significantly reduced the extent of damage; rapid restoration thanks to modular solutions ensured the stability of the power supply

Source: developed by the authors based on United Nations (2024), United Nations Development Programme (2023).

2.4. Electronic warfare and AI-based cybersecurity for protecting Ukraine's energy infrastructure

Electronic warfare played a critically important role in neutralizing drones and guided missiles that relied on radio frequency control or Global Positioning System navigation (United Nations Development Programme 2023). Electronic warfare systems created electromagnetic interference that disrupted the connection between the drone and its operator, causing it to lose orientation or crash prematurely. In Ukraine, electronic warfare devices were actively deployed to protect energy facilities from UAV attacks. For example, portable electronic warfare systems such as "Bukovel-AD" or "Nota" were capable of tracking signals at distances of up to 100 kilometers and jamming signals within a radius of up to 20 kilometers, thereby effectively neutralizing drones before the drones could reach the target. In addition, electromagnetic guns were being developed to generate powerful pulses that could disable the electronics of hostile UAVs. Such systems proved especially valuable during mass attacks, when dozens of drones were launched simultaneously, as the systems allowed multiple targets to be affected at once.

In 2024, Ukraine began integrating electronic warfare systems with monitoring systems combining acoustic sensors and radar to accurately detect drones, significantly improving defense effectiveness (Costanzo et al. 2024). Integration and automation were also important aspects of modern active defense systems. To enhance the effectiveness of air defense, interceptor drones, and electronic warfare, these systems were integrated into a single network comprising radars, acoustic sensors, thermal imagers, and software for coordination.

In Ukraine, early warning systems combining radar data with acoustic sensors were employed to detect drones at distances of several kilometers. This data was transmitted to fire teams or electronic warfare systems, enabling a rapid response to threats. Automated platforms, such as battle management systems, were also used to synchronize the actions of various defense assets – particularly critical during mass attacks, when dozens of drones or missiles might be involved simultaneously (Nikitin 2025). An important factor that also required attention was the increasing dependence of critical energy infrastructure facilities on digital control systems, particularly automated SCADA systems, which ensured real-time monitoring and management (Cybersecurity and Infrastructure Security Agency 2021; Ilves 2025; Cybersecurity in the… 2025).

Although this digital transformation improved operational efficiency and flexibility, it also rendered these facilities vulnerable to cyberattacks that could disrupt energy supply, cause economic losses, or even threaten national security. In Ukraine, since 2022, Russian cyberattacks on the energy infrastructure have become part of hybrid warfare, making cybersecurity one of the critically important elements of national security.

Modern cybersecurity technologies – including artificial intelligence (AI), machine learning, network segmentation, and the implementation of international standards – enabled effective responses to cyberthreats. These technologies and the application for protecting critical energy infrastructure facilities were considered in detail below (Kravchuk et al. 2024).

Artificial intelligence and machine learning played a leading role in modern cybersecurity for energy facilities, allowing for prompt detection and response to threats in the context of rapidly evolving cyberattacks (Cybersecurity and Infrastructure Security Agency 2021; Ilves 2025; Cybersecurity in the… 2025). AI was used to monitor anomalies in the operation of SCADA systems, which formed the basis of digital control for energy facilities. Unusual login attempts, unexpected orders, or departures from standard operating procedures are examples of suspicious patterns that set off alarms for prompt cybersecurity team response. Among the mitigation strategies were patch deployment, multifactor authentication, automatic isolation of impacted network parts, and incident response procedures coordinated with both domestic and foreign partners (Shchuka 2025). Even with these precautions, there are still systemic weaknesses, especially in old software, obsolete technology, and staff members' inability to handle concurrent multi-vector attacks. Furthermore, the risks of coordinated hybrid attacks, which mix physical and cyberattacks, cannot be completely eliminated by integrating AI, leaving vital infrastructure vulnerable to highly skilled adversaries.

Machine learning, in turn, enabled protection systems to adapt to new and constantly evolving threats. Machine learning algorithms were trained on historical data about cyberattacks, allowing for the forecasting of potential vulnerabilities and automatically updating protective mechanisms.

Cyberattacks on Ukraine's energy system demonstrated the seriousness of the threats (Chaika 2023; Grigorska 2023). For example, on October 10–12, 2022, the Russian hacker group Sandworm launched cyberattacks on SCADA substation control systems, exploiting vulnerabilities to disable automatic breakers. These attacks coincided with massive missile strikes on the energy infrastructure on October 10, 2022, intensifying the effect.

The hackers had infiltrated the system back in June 2022, carefully studying its weak points, which led to unplanned power outages in several regions and complicated the functioning of critical infrastructure, including water supply and heating. The combination of cyberattacks and physical strikes resulted in temporary blackouts that affected thousands of consumers (Telbayeva et al. 2023).

Another example was the December 2021 attack on the control systems of NEC "Ukrenergo". Hackers linked to Russian special services conducted a targeted attack on Ukrenergo's automated process control systems, attempting to disable substations in several regions. The attack used malicious software to disrupt the functioning of SCADA systems, which could have caused power outages. This attack was considered a preparatory stage for a broader campaign preceding the full-scale invasion of 2022.

Although the attack was detected before it caused significant disruptions, it exposed vulnerabilities in the cybersecurity systems, in particular, inadequate network segmentation and outdated software. This was why AI-based systems were actively implemented to protect key facilities, including through cooperation with international partners such as the USA and the EU.

2.5. Decentralization, AI, and international lessons for resilient energy infrastructure in Ukraine

One of the fundamental cybersecurity approaches that enabled minimization of cyberattack propagation in the event of a breach was network segmentation. This method involved dividing a facility's digital infrastructure into isolated segments, each with its own protection mechanisms and limited access to other network parts. For instance, SCADA control networks were separated from administrative networks used for office tasks to prevent malware intrusion via less secure entry points, such as email or staff workstations.

Modern energy operators, such as NEC "Ukrenergo", actively applied segmentation, combining it with other measures such as data encryption and multifactor authentication. It should be noted that international standards and regulatory frameworks played a key role in systematizing and improving the level of cybersecurity for energy facilities. The introduction of standards ISO/IEC No. 27001:2022 "Information Security Management Systems" (2022) and the National Institute of Standards and Technology (2025) helped create comprehensive protection systems covering all aspects – from risk assessment to incident response. These standards included regular audits, vulnerability testing, and personnel training, which were particularly important in the context of increasing cyberattack complexity. In Ukraine, the cybersecurity of critical energy infrastructure facilities was also regulated by national rules, particularly the Resolution of the Cabinet of Ministers of Ukraine No. 518 "On Approval of the General Requirements for Cyber Defence of Critical Infrastructure Facilities" (2019). These requirements set out mandatory measures for critical infrastructure operators, including monitoring system implementation, critical network isolation, and coordination with state bodies such as the State Special Communications Service. In addition, Ukraine cooperated with NATO and the European Union Agency for Cybersecurity to adapt the world's best practices to local conditions.

Decentralization and reserve capacity of energy systems also remained important elements in ensuring the resilience of Ukraine's critical infrastructure under combat conditions (United Nations Development Programme 2023). Decentralized small distribution systems – including small power stations, solar panels, wind turbines, and battery storage systems – enabled the creation of local energy hubs that provided backup power to critical facilities such as hospitals, military bases, or command centers, even in cases where the main grid was damaged (Voitenko and Polishchuk 2025). Reserve schemes, such as duplicate transmission lines and protected control points, were developed in parallel to bypass damaged sections of the network. Mobile energy units, including portable generators and compact transformers, played a key role in the rapid restoration of power supply (Hotra et al. 2024; Golub et al. 2018; Langella et al. 2016).

After the attacks during the winter of 2022–2023, the EU and the United States delivered hundreds of such devices to Ukraine, which helped to promptly restore electricity supply to hospitals and water utilities in affected regions. These measures significantly reduced the vulnerability of the energy system to attacks, but the implementation was hindered by limited

financial resources, logistical challenges, and the need for coordination between government bodies, private operators, and international partners.

Innovative materials and technologies additionally played an important role in enhancing resilience and accelerating the restoration of Ukraine's critical energy infrastructure – especially in conditions where damage to equipment caused by missile and drone attacks became a systemic issue. One of the most promising solutions was 3D printing, which enabled the production of spare parts for energy equipment directly on site, significantly speeding up repair operations.

In Ukraine, logistics chains were frequently disrupted by military operations, and access to imported components was limited, making 3D printers an effective tool for quickly reproducing complex parts from metal, plastic, or composite materials – reducing facility downtime from weeks to hours. For example, in 2023, Ukrainian energy companies began using industrial 3D printers to manufacture spare parts for damaged substations, supported by international partners (Babak and Kulyk 2023).

Another important solution was modular transformers, which were characterized by compactness, ease of transport, and quick installation, making the transformers ideal for replacing damaged units in combat zones. Unlike traditional transformers, which could weigh dozens of tonnes and require complex logistics, modular transformers could be transported by truck and installed within a few hours, which was critical for restoring electricity in affected regions (Ashirbaev 2021; Ashirbaev et al. 2023).

In Ukraine, such transformers had been actively used since 2022 as part of humanitarian deliveries from the EU, which included hundreds of compact units to replace those destroyed by Russian strikes. In particular, the supply of modular transformers was carried out by Lithuania, Latvia, Estonia, Poland, and Germany. For instance, Lithuania delivered dozens of compact transformers for substations in 2022, and Poland coordinated the logistics for the delivery of hundreds of units through its warehouses under the EU4Energy program (International Energy Agency 2025). In total, between 2022 and 2023, approximately 1,800 transformers of varying capacity were delivered by EU countries, a significant portion of which were modular models.

A critical initiative was the Decision of the National Security and Defense Council of Ukraine "On the Organization of Protection and Ensuring the Security of the Functioning of Critical Infrastructure and Energy Facilities of Ukraine in the Context of Military Operations" (2023), which defined a comprehensive approach to strengthening the protection of critical infrastructure facilities. This document provides for multilayered protection, including engineering solutions such as the construction of concrete fortifications and modular shelters to safeguard substations and transformers from missile strikes and kamikaze drones. This was a direct response to the massive attacks of 2022–2023 that caused prolonged blackouts.

Anti-drone systems – including nets, electronic warfare devices, and interceptor drones – were being actively deployed to neutralize UAVs. Backup energy supply – including portable generators and modular transformers – became critically important for the rapid restoration of electricity after strikes. The modernization of critical infrastructure object categorization methodologies, as provided for in the decree, aimed to clearly define protection priorities, which made it possible to optimize resource distribution. For example, in 2023, the classification of

facilities was revised to include small distributed energy sources, such as solar panels, in the critical infrastructure list – thereby contributing to decentralization. These initiatives, supported by international partners, demonstrated Ukraine's progress in building a resilient energy system. However, the implementation was complicated by limited finances, a shortage of specialists, and the need for rapid adaptation to constantly evolving new threats.

International experience and standards for the protection of critical energy infrastructure also influenced the formation of Ukraine's strategies, as the country adapted advanced approaches to counter threats in wartime conditions and integrate into European energy markets. The key approaches, technologies, and standards used in other countries to counter hybrid threats were presented in Table 2.

Table 2. Key approaches, technologies, and standards used in other countries to counter hybrid

Tabela 2. Główne strategie, technologie i normy stosowane w innych krajach w walce z zagrożeniami hybrydowymi

Country/ region	Basic approaches to protection	Technologies and solutions	Standards and directives
EU (Germany, Baltic countries)	The concept of infrastructure resilience, emphasis on decentralization of energy systems and cyber defense	Distributed energy sources (solar and wind installations) to reduce dependence on large power plants; network segmentation for cyber defense	NIS2 Directive, European Union Agency for Cybersecurity standards for mandatory cybersecurity and network protection audits
USA	Using AI to predict attacks, modular power systems for rapid recovery	AI systems (e.g., Pacific Northwest National Laboratory) to predict SCADA system vulnerabilities with up to 98% accuracy; mobile generators and compact transformers for disaster recovery	National Institute of Standards and Technology SP 800-53 for cybersecurity, FEMA standards for physical security
Israel	Advanced defense against missile and drone attacks, emphasis on active defense and electronic warfare	Iron Dome air defense system (intercepts up to 90% of missiles); electronic warfare systems for jamming Global Positioning System and drone radio signals	Own standards for cybersecurity (INACS) and physical security

Source: developed by the authors based on NIS2 Directive "Securing Network and Information Systems" (2023), European Union Agency for Cybersecurity (2025), National Institute of Standards and Technology (2020), International Trade Administration (2025), The U.S.-Israel Cybersecurity (2021), Tabansky (2025), Pacific Northwest National Laboratory (2025).

These examples demonstrate how international experience and standards can be adapted by Ukraine to create a resilient energy system capable of withstanding hybrid threats. Ukraine has already effectively incorporated a number of the lessons learned from the global models shown in Table 2, especially with regard to decentralization and quick energy system recovery. Ukraine

has adopted small-scale solar panels, wind turbines, and battery storage systems to establish local energy hubs that can independently power vital facilities, like hospitals and military bases, even in the event that the main grid is disrupted. This initiative was motivated by the EU's emphasis on distributed energy sources. Using the USA as a model, AI-based monitoring systems have been implemented to anticipate and identify assaults on SCADA networks, facilitating improved emergency intervention coordination and quicker threat responses. Israel's emphasis on electronic warfare and active defense has influenced the deployment of interceptor drones, electronic jamming devices, and anti-drone systems to counter UAV threats.

In reality, these modifications differ from the original models because of Ukraine's resource limitations and wartime situation. The US and EU methods are predicated on a solid infrastructure and a wealth of resources, but Ukraine has modified these strategies to function in the face of ongoing attacks, scarce finances, and disrupted supply chains. Due to personnel constraints, AI monitoring systems are merged with manual oversight, decentralized energy hubs are smaller and can be deployed more quickly than their EU counterparts, and active defense systems are frequently transportable and modular rather than permanent installations like Israel's Iron Dome. These changes demonstrate a practical, situation-specific methodology that strikes a balance between the operational realities of a nation engaged in hybrid warfare and the theoretical advantages of international models.

2.6. Challenges and strategic recommendations for protecting Ukraine's energy infrastructure

It should be emphasized that the implementation of innovative technologies for the protection of energy-related critical infrastructure in Ukraine faces significant challenges that hinder the rapid and effective deployment of modern solutions. Table 3 presents the main challenges, describing the nature as well as the impact on the implementation of technologies.

Thus, the analysis of existing challenges demonstrated that the successful implementation of innovative technologies for the protection of energy-related critical infrastructure in Ukraine requires a systematic approach that combines financial support, personnel training, rapid response, and effective coordination. Based on the conducted analysis, recommendations for strengthening the energy system to ensure resilience and rapid recovery after attacks were proposed and are presented in Figure 2.

Strengthening physical protection remained a top priority, as energy facilities continued to be primary targets of missile and drone attacks. The expansion of second-tier concrete fortifications, which began in Ukraine in 2023, had to be scaled up to cover all key critical infrastructure facilities, including small distribution stations. These structures, reinforced with rebar frameworks, provided protection against shrapnel and blast waves, reducing the risk of damage. At the same time, it was necessary to increase the deployment of anti-drone systems such as nets, electronic warfare complexes, and mobile fire units with man-portable air defense

Table 3. Challenges of implementing innovative technologies for protecting energy facilities of the critical infrastructure

Tabela 3. Wyzwania związane z wdrażaniem innowacyjnych technologii służących ochronie obiektów energetycznych infrastruktury krytycznej

Challenge	Description	Influence
Financing	The implementation of technologies such as AI, electronic warfare, 3D printing, or modular systems requires significant capital investments, which are limited due to war and economic difficulties	Delays in the deployment of modern systems, dependence on international assistance
Staff shortage	The lack of cybersecurity specialists, engineers for working with electronic warfare, AI, or 3D printers complicates the operation and maintenance of systems	Limited ability to use technology effectively, risk of errors
Response speed	Constant attacks require instant deployment of technology, but logistics and bureaucracy slow down the process	Increased downtime after attacks, risk of blackouts
Coordination	The lack of clear interaction between government agencies, critical infrastructure operators, and international partners reduces efficiency	Inefficient use of resources, duplication of efforts, delays in funding

Source: developed by the authors based on United Nations (2024), United Nations Development Programme (2023).

systems to neutralize Shahed-136. To implement this, additional funding through the state budget and international grants was required, as well as the simplification of logistical procedures for the rapid deployment of equipment in combat zones.

Cybersecurity development was critically important due to the growing dependence of energy facilities on digital control systems such as SCADA, which were vulnerable to cyberattacks. The implementation of AI-based monitoring systems capable of detecting network traffic anomalies and forecasting attacks could significantly improve security. After the 2022–2023 attacks, Ukraine had already begun cooperating with the United States to integrate such systems, but the use had to be extended to all critical infrastructure facilities.

Compliance with international standards ISO/IEC No. 27001:2022 "Information Security Management Systems" (2022) and the Cybersecurity Framework of the National Institute of Standards and Technology (2025), along with national regulations, would ensure a systematic approach to protection, including network segmentation and regular audits. This required investment in software, the establishment of cybersecurity centers, and partnerships with organizations such as the European Union Agency for Cybersecurity to adapt European practices.

Decentralizing the energy system was a strategic move to reduce vulnerability to attacks, as the failure of a single facility in a centralized system could result in a regional blackout. Investment in small distribution systems such as solar panels, wind turbines, and battery storage would allow the creation of local energy hubs capable of autonomously powering critical facilities like hospitals or military bases.

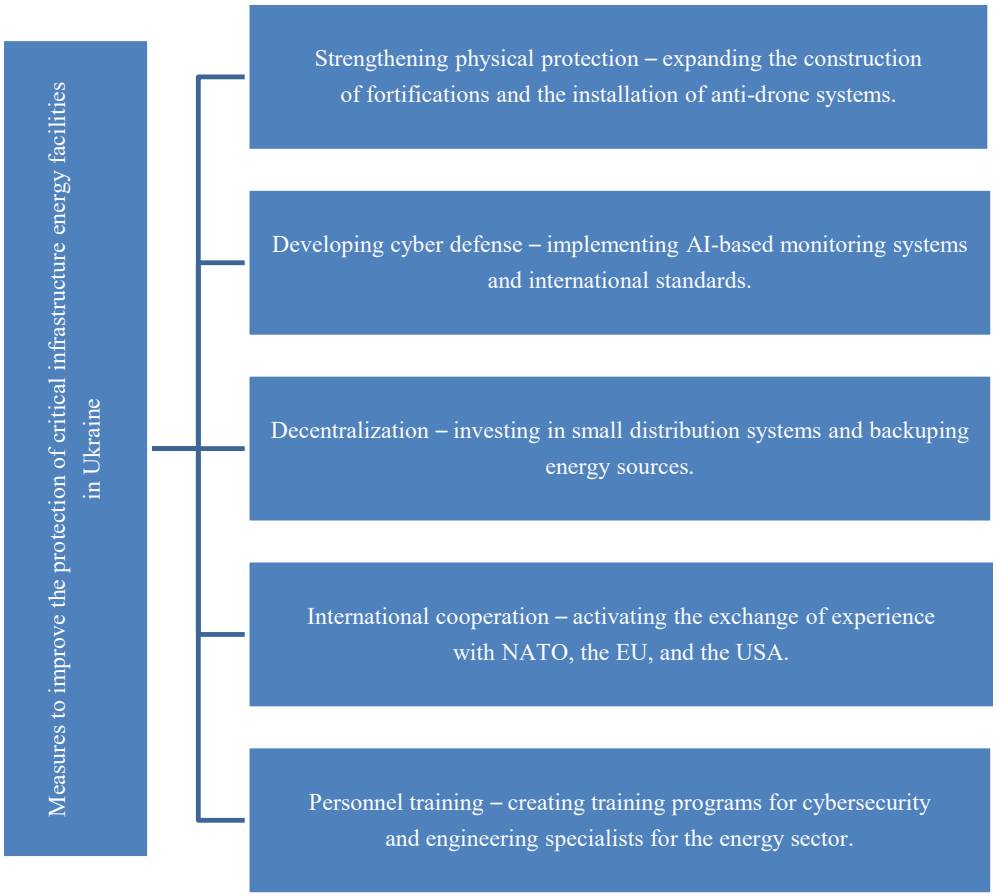

Fig. 2. Recommendations for the protection of critical infrastructure energy facilities in Ukraine
Source: developed by the authors

Rys. 2. Zalecenia dotyczące ochrony obiektów infrastruktury energetycznej o znaczeniu krytycznym w Ukrainie

Programs such as the U.S. Agency for International Development (2025) already supported such initiatives, but the scale had to be increased, especially in frontline regions. Backup energy sources, including modular transformers and mobile generators supplied to Ukraine by the EU and US after the 2022–2023 attacks, had to be integrated into a unified rapid response system (International Energy Agency 2025). This required the development of a national decentralization strategy, involvement of the private sector, and financing through international funds.

In turn, international cooperation was fundamental for the rapid implementation of advanced technologies and practices. Strengthening experience-sharing with NATO, the EU, and the US could accelerate the adoption of solutions such as the EU's resilience concept, AI-based attack prediction systems from the US, or Israeli anti-drone technologies (electronic warfare and air defense systems like the "Iron Dome"). Initiatives, including joint exercises, technical assistance,

and equipment deliveries, needed to be expanded. The creation of coordination centers with partners would optimize resource allocation and prevent inefficient use.

Training personnel was critical for the effective use of complex technologies, as the shortage of specialists in cybersecurity, electronic warfare engineering, or 3D printing limited the application. Establishing national training programs, for instance, in cooperation with universities and international organizations, would enable the preparation of specialists to operate AI systems, electronic warfare complexes, and modular energy units. Short-term courses supported by partners could quickly enhance the qualifications of critical infrastructure operators. In the long term, it was necessary to invest in educational programs in cybersecurity and energy engineering to create a workforce capable of responding to modern threats.

The launch of training centers in 2023 for operating electronic warfare systems had already shown positive results, but the number and coverage required expansion. The implementation of these recommendations demanded a comprehensive approach, combining national efforts with international support.

Strengthening physical and cyber protection would ensure immediate resilience to attacks, while decentralization and backup solutions would form the basis for long-term security. International cooperation and personnel training would address gaps in resources and qualifications, enabling Ukraine not only to withstand current threats but to build a modern energy system integrated into European standards.

3. Discussion

As a result of this study, it was established that the means of physical protection for energy critical infrastructure facilities in Ukraine – which include both active (local air defense systems, electronic warfare complexes, anti-drone nets, acoustic sensors, mobile fire units with man-portable air defense systems) and passive (second-level concrete fortifications, underground facilities, backup power lines) measures – proved effective in neutralizing physical threats, including Shahed-136 UAVs and missile attacks.

In the study by Pietrek (2022), multi-component anti-drone systems were examined, including radars, laser effectors, and electronic warfare, aimed at active critical infrastructure protection, but with insufficient attention paid to passive measures such as fortifications, which are critically important for comprehensive protection in wartime conditions, where economic constraints necessitate a combination of active and passive methods. The article by Zmysłowski et al. (2023) focused on the integration of electronic warfare with high-tech radars for active drone protection, which aligns with this study's findings on the need for a combined approach but ignores passive measures, which were identified as key to power system resilience during intensive attacks.

In the study by Park et al. (2021), a review of anti-drone systems using electronic warfare, acoustic, and infrared sensors for active protection was conducted, which is consistent with this

study's conclusions, but it did not consider passive solutions, which were deemed important for defense against attacks. The work by Piekarski et al. (2025) analyzed hybrid UAV threats with cyber elements and proposed AI for effective attack forecasting, which partially coincides with the idea of integrating active means, but did not cover passive measures, which in this study were defined as essential for protection against physical damage. The study by Dudenhoeffer (2020) highlighted the effectiveness of early warning through sensor networks for active drone defense, in line with this study's conclusions, but did not account for passive fortifications, which are an essential part of protection in wartime conditions.

The article by Linger et al. (2021) emphasized the role of underground fortifications as passive defense, which fully aligns with this study's recommendations, but did not include an analysis of active means, which are necessary for a comprehensive approach. The study by Łukasiewicz (2020) focused on the protection of nuclear facilities through air defense and physical fortifications, which coincides with this study's conclusions regarding combining active and passive means, but did not consider flexibility and speed of deployment, which are crucial under wartime conditions in Ukraine. Thus, this study stands out for its comprehensive approach covering both active and passive means of physical protection adapted to the wartime context in Ukraine, while the cited works partially align with the conclusions but focus either on active or passive measures, offering less flexible or more theoretical solutions.

In the course of this study, it was determined that the cyber protection of energy critical infrastructure facilities – based on the implementation of AI-based monitoring systems, network segmentation, ISO/IEC No. 27001:2022 "Information Security Management Systems" (2022), and rapid incident response – may effectively reduce vulnerability to cyberattacks, although it requires adaptation to hybrid threats that combine cyber and physical attacks. In the study by Alcántara Suárez and Monzon Baeza (2023), the role of machine learning in defense systems was emphasized, particularly for cyber threat forecasting, which aligns with the conclusions regarding AI monitoring but focuses on general defense applications with less detail on the specifics of the energy sector.

The work by Govea et al. (2024) demonstrated the high effectiveness of AI in energy-critical infrastructure cyber defense, particularly through big data analysis to detect anomalies, which confirms the findings of this study but does not consider practical constraints such as resource shortages in Ukraine. In the study by Chehri et al. (2021), risk assessment models for smart grids using big data and AI were proposed, consistent with conclusions on the importance of predictive analytics, but ignoring hybrid threats, which are critical in the Ukrainian context due to combined physical and cyberattacks. The study by Ojo et al. (2024) focused on innovative solutions such as blockchain and AI for protection against cyber-physical attacks, partially aligning with this study's recommendations, but less adapted to the military conditions characteristic of Ukraine.

The work by Alqudhaibi et al. (2023) presented a proactive approach to cyber threat forecasting based on attacker motivations, complementing the conclusions on AI monitoring, but the focus on Industry 4.0 limits applicability to energy systems; standards like ISO/IEC were also emphasized. The study by Wisniewski et al. (2022) systematically analyzed the impact of Industry 4.0 on critical infrastructure security, highlighting the role of AI, partially aligning with

this study's conclusions but not accounting for the specifics of hybrid warfare, which is central to this study.

The research by Yu et al. (2021) focused on identifying threats in industrial IoT using deep learning, confirming AI effectiveness in cyber defense, but with less emphasis on integration with physical measures, which was deemed essential for Ukraine due to frequent missile attacks. Thus, this study is distinguished by its focus on practical adaptation of cyber protection to wartime conditions, combining AI with economically viable solutions and attention to hybrid threats, whereas the cited works partially align with the conclusions but offer less contextually adapted solutions. This study also noted that innovative technologies – particularly 3D printing for producing spare parts for energy equipment and modular transformers for rapid power restoration – play an important role in improving the resilience of energy critical infrastructure, allowing for reduced repair time, although large-scale implementation still requires integration into logistics networks.

In the study by Khan and Koc (2024), the energy efficiency of 3D printing for producing protective materials for critical infrastructure was highlighted, which aligns with the study's findings on rapid component fabrication but with a focus on protective materials rather than energy equipment, whereas this study examined the use of 3D printing for transformers and turbines under wartime conditions. The work by Budzik et al. (2022) analyzed the possibilities of 3D printing for critical infrastructure, particularly for spare parts and modular structures, fully confirming this study's results, but without considering the military context where speed and mobility are critically important.

The study by Soldatos et al. (2020) proposed integrated cyber-physical protection, including modular technologies for rapid restoration, partially coinciding with this study's conclusions but with an emphasis on cyber protection, limiting the analysis of physical innovations, which are also important. In the study by Qudus (2025), modular systems were described as the foundation for critical infrastructure resilience against cyber-physical threats, aligning with the results of this study, but without detailing 3D printing, which is promising for local production. The study by Topor (2023) focused on electronic warfare as an innovative technology, ignoring 3D printing and modular transformers, which differ from the comprehensive approach of this study, where these technologies were considered for restoration. The work by Pătraşcu (2021) analyzed the impact of IoT on critical infrastructure protection, which is less relevant to this study's conclusions about the central role of 3D printing and transformers in wartime.

In the study by Papadopoulos et al. (2024), an integrated approach to protection from cyber-physical threats was proposed, including modular technologies, which aligns with the results of this study, but the focus on the European context is less adapted to the extreme conditions of war than the practical recommendations in this research. Thus, this study is characterized by its emphasis on the practical use of 3D printing and modular transformers in Ukraine's wartime context, whereas the cited works partially align with the findings but focus on broader or less specific applications, overlooking the unique challenges of war.

Therefore, the analysis of this study's results in conjunction with those of the cited works highlighted the importance of a comprehensive approach to protecting energy-critical

infrastructure facilities that combines physical protection, cybersecurity, and innovative technologies. These studies point to the need for adapting modern solutions to specific conditions, such as wartime, where speed of implementation and economic viability are critically important. This approach not only enables effective counteraction to hybrid threats but also ensures rapid recovery of the power system after attacks, which is essential for maintaining societal functioning under wartime conditions.

Conclusions

As a result of this study, it was established that protecting energy-critical infrastructure facilities in Ukraine is a complex task requiring a combination of innovative technologies, international experience, strategic planning, and rapid response in wartime. It was noted that in 2021, Ukraine's electricity generation capacity stood at 53.3 GW, and electricity production reached 158.4 billion kWh. Since February 2022, when Russia began systematic attacks on energy infrastructure, Ukraine has lost about two-thirds of its generation capacity before full-scale war (down to ~15.4 GW by mid-2024), highlighting the critical need for resilient solutions.

The study highlighted key aspects of protecting energy critical infrastructure in Ukraine, emphasizing the effectiveness of active protection, cyber defense, decentralization, and innovative technologies in ensuring energy system resilience under wartime conditions. It was found that active protection shows high effectiveness in neutralizing threats such as Shahed-136 UAVs and missiles due to the deployment of local air defense systems, electronic warfare (notably "Bukovel-AD" complexes), and anti-drone technologies, including mobile fire units and interceptor drones.

Cyber protection, supported by AI-based monitoring systems capable of detecting anomalies in SCADA systems with high accuracy, plays a critical role in countering cyberattacks, ensuring the security of digital control systems and the resilience to complex threats. Modern technologies, particularly 3D printing and modular transformers, revolutionize recovery processes: 3D printers allow rapid production of spare parts for equipment, and compact modular transformers, easily transportable and installable, ensure quick restoration of power supply after attacks.

International experience from the EU, USA, and Israel offers resilience models that Ukraine is adapting, although the war complicates full implementation. Major challenges remain: funding, staff shortages, response speed, and coordination. To overcome these, the study proposes recommendations: strengthening physical protection through fortifications and anti-drone systems; developing cyber defense with an AI focus; decentralization via investment in distributed systems; enhanced cooperation with NATO, the EU, and the USA; and creating specialist training programs. For future research, promising directions include experimental

testing of innovative technologies such as quantum computing for cyber defense and autonomous restoration systems, with assessment of the economic feasibility and effectiveness under hybrid threat conditions.

The Authors have no conflicts of interest to declare.

References

Alcántara Suárez, E.J. and Monzon Baeza, V. 2023. Evaluating the role of machine learning in defense applications and industry. *Machine Learning and Knowledge Extraction* 5(4), pp. 1557–1569, https://doi.org/10.3390/make5040078.

Alqudhaibi et al. 2023 – Alqudhaibi, A., Albarrak, M., Aloseel, A., Jagtap, S. and Salonitis, K. 2023. Predicting cybersecurity threats in critical infrastructure for industry 4.0: A proactive approach based on attacker motivations. *Sensors* 23(9), https://doi.org/10.3390/s23094539.

Ashirbaev et al. 2023 – Ashirbaev, B., Altymyshova, Z. and Alymbaeva, Z. 2023. Optimal Energy-Saving Control for a Thermal Plant of a Linear Singularly Perturbed Discrete System with a Small Step. In *International Conference on Electrical, Computer and Energy Technologies, ICECET 2023*. Cape Town: Institute of Electrical and Electronics Engineers, https://doi.org/10.1109/ICECET58911.2023.10389496.

Ashirbaev, B.Y. 2021. Solving the problem of analytical design of the controller for a stationary discrete system with a small step. *Journal of Physics: Conference Series* 1864(1), https://doi.org/10.1088/1742-6596/1864/1/012030.

Babak et al. 2021 – Babak, V.P., Scherbak, L.M., Kuts, Y.V. and Zaporozhets, A.O. 2021. Information and measurement technologies for solving problems of energy informatics. *CEUR Workshop Proceedings* 3039, pp. 24–31.

Babak, V.P. and Kulyk, M.M. 2023. Increasing the efficiency and security of integrated power system operation through heat supply electrification in Ukraine. *Science and Innovation* 19(5), pp. 100–116, https://doi.org/10.15407/scine19.05.100.

Budzik et al. 2022 – Budzik, G., Tomaszewski, K. and Soboń, A. 2022. Opportunities for the application of 3D printing in the critical infrastructure system. *Energies* 15(5), https://doi.org/10.3390/en15051656.

Chaika, O. 2023. Russian hackers are coordinating with the military and stepping up attacks ahead of winter. How Ukraine is countering cyberattacks on the energy system (*Rosiys'ki khakery koordynuyut' diyi z viys'kovymy ta posylyuyut' ataky naperedodni zymy. Yak Ukrayina protystoyit' kiberatakam na enerhosystemu*). [Online:] https://forbes.ua/company/rosiyski-khakeri-koordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberatakam-na-energosistemu-08112023-17242 [Accessed: 2026-02-08] (*in Ukrainian*).

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

Costanzo et al. 2024 – Costanzo, L., Rubino, G., Rubino, L. and Vitelli, M. 2024. PFC Control Signal Driven MPPT Technique for Grid-Connected PV Systems. *IEEE Transactions on Power Electronics* 39(8), pp. 10368–10379, https://doi.org/10.1109/TPEL.2024.3393294.

Cybersecurity and Infrastructure Security Agency 2021. Cyber-Attack Against Ukrainian Critical Infrastructure. [Online:] https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [Accessed: 2026-02-08].

Cybersecurity in the Power Sector 2025. [Online:] https://www.eurelectric.org/in-detail/cybersecurity-in-the-power-sector/ [Accessed: 2026-02-08].

Decision of the National Security and Defense Council of Ukraine "On the Organization of Protection and Ensuring the Security of the Functioning of Critical Infrastructure and Energy Facilities of Ukraine in the Context of Military Operations" 2023. [Online:] https://www.president.gov.ua/documents/6952023-48641 [Accessed: 2026-02-08] (*in Ukrainian*).

Defense Express 2023. *Drone Hunters are Already Protecting Ukraine's Critical Infrastructure*. [Online:] https://en.defence-ua.com/news/drone_hunters_are_already_protecting_ukraines_critical_infrastructure-5569.html [Accessed: 2026-02-08].

Di Pietro et al. 2021 – Di Pietro, R., Raponi, S., Caprolu, M. and Cresci, S. 2021. Critical infrastructure. In R. Di Pietro, S. Raponi, M. Caprolu and S. Cresci (Eds.), *New Dimensions of Information Warfare*, pp. 157–196, Cham: Springer, https://doi.org/10.1007/978-3-030-60618-3_5.

Dudenhoeffer, D.D. 2020. Day of the drone: protecting critical infrastructure from terrorist use of unmanned aerial systems. [In:] *Toward Effective Cyber Defense in Accordance with the Rules of Law*, pp. 17–31. London: IOS Press, https://doi.org/10.3233/NHSDP200038.

European Union Agency for Cybersecurity 2025. Cybersecurity of Critical Sectors. [Online:] https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors [Accessed: 2026-02-08].

Golub et al. 2018 – Golub, G., Kukharets, S., Tsyvenkova, N., Yarosh, Y. and Chuba, V. 2018. Experimental study into the influence of straw content in fuel on parameters of generator gas. *Eastern-European Journal of Enterprise Technologies* 5(8-95), pp. 76–86, https://doi.org/10.15587/1729-4061.2018.142159.

Govea et al. 2024 – Govea, J., Gaibor-Naranjo, W. and Villegas-Ch, W. 2024. Transforming cybersecurity into critical energy infrastructure: A study on the effectiveness of artificial intelligence. *Systems* 12(5), https://doi.org/10.3390/systems12050165.

Grigorska, N. 2023. From the Ukrainian power grid to the Pentagon. Seven of Russia's biggest cyberattacks in Ukraine and around the world during two years of major warfare. [Online:] https://nv.ua/ukr/ukraine/events/hakerska-ataka-rosiji-na-kijivstar-7-naybilshih-kiberatak-na-ukrajinu-ta-krajini-svitu-pid-chas-viyni-50375741.html [Accessed: 2026-02-08] (*in Ukrainian*).

Hotra et al. 2024 – Hotra, O., Kulyk, M., Babak, V., Kovtun, S., Zgurovets, O., Mroczka, J. and Kisała, P. 2024. Organisation of the Structure and Functioning of Self-Sufficient Distributed Power Generation. *Energies* 17(1), https://doi.org/10.3390/en17010027.

Ilves, I. 2025. Ukraine Teaches Europe Cyber Lessons. [Online:] https://cepa.org/article/ukraine-teaches-europe-cyber-lessons/ [Accessed: 2025-12-08].

International Energy Agency 2025. *EU4Energy*. [Online:] https://www.iea.org/programmes/eu4energy.

International Trade Administration 2025. *Israel Cybersecurity Strategy 2025: A Strategic Gateway for U.S.* [Online:] https://www.trade.gov/market-intelligence/israel-cybersecurity-strategy-2025-strategic-gateway-us [Accessed: 2026-02-08].

Ismanzhanov et al. 2012 – Ismanzhanov, A.I., Murzakulov, N.A. and Azimzhanov, O.A. 2012. Investigation on heat exchange in interlayer space of multilayer greenhouses. *Applied Solar Energy* (*English translation of Geliotekhnika*) 48(2), pp. 118–120, https://doi.org/10.3103/S0003701X12020107.

Ismanzhanov, A.I. and Tashiev, N.M. 2016. Development and research of the technology for powdering agricultural products using solar energy. *Applied Solar Energy* (*English translation of Geliotekhnika*) 52(4), pp. 256–258, https://doi.org/10.3103/S0003701X16040101.

ISO/IEC No. 27001:2022 "Information Security Management Systems" 2022. [Online:] https://www.iso.org/standard/27001 [Accessed: 2025-12-08].

Khan, S.A. and Koc, M. 2024. Advancements in additively manufactured safety materials: Energy-efficient 3D printing solutions for critical infrastructure. *ASME International Mechanical Engineering Congress and Exposition* Proceedings Series, https://doi.org/10.1115/IMECE2024-140326.

Knapik, M. 2017. Analysis of the possibility to cover energy demand from renewable sources on the motive power of the heat pump in low-energy building. *E3S Web of Conferences* 17, https://doi.org/10.1051/e3sconf/20171700039.

Kootala et al. 2023 – Kootala, A., Mousa, A. and Pong, P.W. 2023. Drones are endangering energy critical infrastructure, and how we can deal with this. *Energies* 16(14), https://doi.org/10.3390/en16145521.

Koval et al. 2022 – Koval, M.V., Koval, V.V., Kotsyuruba, V.I. and Bilyk, A.S. 2022. Organizational and technical principles of building a system of engineering protection of critical infrastructure of the energy sector of Ukraine. *Science and Defense* 3(4), pp. 11–16, https://doi.org/10.33099/2618-1614-2022-20-3-4-11-16.

Kravchuk et al. 2024 –Kravchuk, M., Kravchuk, V., Hrubinko, A., Podkovenko, T. and Ukhach, V. 2024. Cyber security in Ukraine: Theoretical view and legal regulation. *Law, Policy and Security* 2(2), pp. 28–38, https://doi.org/10.62566/lps/2.2024.28.

Kubiczek et al. 2023 – Kubiczek, J., Hadasik, B., Krawczyńska, D., Przedworska, K. and Ryczko, A. 2023. Going beyond frontiers in household energy transition in Poland—a perspective. *Frontiers in Energy Research* 11, https://doi.org/10.3389/fenrg.2023.1239115.

Langella et al. 2016 – Langella, R., Marino, P., Rubino, G., Rubino, L., Testa, A. and Liccardo, F. 2016. Supervision of ancillary services for distributed active front-end in a small industrial AC microgrid. [In:] *2016 International Symposium on Power Electronics, Electrical Drives, Automation and Motion, SPEEDAM 2016*, pp. 308–314. Capri: Institute of Electrical and Electronics Engineers, https://doi.org/10.1109/SPEEDAM.2016.7526032.

Lehto, M. 2022. Cyber-attacks against critical infrastructure. In M. Lehto and P. Neittaanmäki (Eds.), *Cyber Security: Critical Infrastructure Protection*, pp. 3–42. Cham: Springer, https://doi.org/10.1007/978-3-030-91293-2_1.

Linger et al. 2021 – Linger, D.A., Baker, G.H. and Little, R.G. 2021. Applications of underground structures for the physical protection of critical infrastructure. [In:] L. Ozdemir (Ed.), *North American Tunneling 2002*, pp. 333–339. London: CRC Press, https://doi.org/10.1201/9781003211341.

Liubovetskyi et al. 2025 – Liubovetskyi, O.V., Rykhva, V.V. and Bosak, G.S. 2025. Ensuring the protection and functioning of critical infrastructure facilities in modern warfare. [In:] *Civil Protection in Warfare: Collection of Abstracts of the I International Scientific and Practical Conference*, pp. 125–126. Lviv: Lviv State University of Life Safety.

Łukasiewicz, J. 2020. Unmanned aerial vehicle as a device supporting the physical protection system of critical infrastructure facilities: Nuclear power plant as a case in point. *Zeszyty Naukowe. Transport/Politechnika Śląska* 108, pp. 121–131, https://doi.org/10.20858/sjsutst.2020.108.11.

Manuilov, Y.S. 2023. Ensuring cybersecurity of critical infrastructure in the context of cyber warfare. *Information and Law* 44(1), pp. 154–167, https://doi.org/10.37750/2616-6798.2023.1(44).287780.

Marignetti et al. 2023 – Marignetti, F., Di Stefano, R.L., Rubino, G. and Giacomobono, R. 2023. Current Source Inverter (CSI) Power Converters in Photovoltaic Systems: A Comprehensive Review of Performance, Control, and Integration. *Energies* 16(21), https://doi.org/10.3390/en16217319.

Ministry of Energy of Ukraine 2025. Statistical information. [Online:] https://www.mev.gov.ua/taxonomy/term/111 [Accessed: 2025-12-08].

National Institute of Standards and Technology 2020. Security and Privacy Controls for Information Systems and Organizations. [Online:] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final [Accessed: 2025-12-08].

National Institute of Standards and Technology 2025. Cybersecurity Framework. [Online:] https://www.nist.gov/cyberframework [Accessed: 2025-12-08].

NEC "Ukrenergo" 2025. Reports. [Online:] https://ua.energy/about_us/reporting/management-reports/ [Accessed: 2025-12-08].

Nikitin, Y. 2025. Combined energy production systems with Stirling engines: Analysis of global experience and local prospects. *Technologies and Engineering* 26(3), pp. 66–76, https://doi.org/10.30857/2786-5371.2025.3.5.

NIS2 Directive "Securing Network and Information Systems" 2023. [Online:] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive [Accessed: 2025-12-08].

Ojo et al. 2024 – Ojo, B., Ogborigbo, J.C. and Okafor, M.O. 2024. Innovative solutions for critical infrastructure resilience against cyber-physical attacks. *World Journal of Advanced Research and Reviews* 22(3), pp. 1651–1674, https://doi.org/10.30574/wjarr.2024.22.3.1921.

Pacific Northwest National Laboratory 2025. About. [Online:] https://www.pnnl.gov/about [Accessed: 2025-12-08].

Papadopoulos et al. 2024 – Papadopoulos, L., Demestichas, K., Muñoz-Navarro, E., Hernández-Montesinos, J.J., Paul, S., Museux, N., Konig, S., Schauer, S., Alarcon, A.C., Llopis, I.P., Stelkens-Kobsch, T., Hadjina, T. and Levak, J. 2024. Protection of critical infrastructures from advanced combined cyber and physical threats: The PRAETORIAN approach. *International Journal of Critical Infrastructure Protection* 44, https://doi.org/10.1016/j.ijcip.2023.100657.

Park et al. 2021 – Park, S., Kim, H.T., Lee, S., Joo, H. and Kim, H. 2021. Survey on anti-drone systems: Components, designs, and challenges. *IEEE Access* 9, pp. 42635–42659, https://doi.org/10.1109/ACCESS.2021.3065926.

Pătrașcu, P. 2021. Emerging technologies and national security: The impact of IoT in critical infrastructures protection and defence sector. *Land Forces Academy Review* 26(4), pp. 423–429, https://doi.org/10.2478/raft-2021-0055.

Piekarski et al. 2025 – Piekarski, M., Wolbach, M. and Okuniewska, M. 2025. Employment of uncrewed systems in attacks on critical infrastructure: A hybrid threat perspective. *Open Research Europe* 4, article number 129, https://doi.org/10.12688/openreseurope.17797.1.

Pietrek, G. 2022. Critical infrastructure security management anti-drone systems. *Wiedza Obronna* (3), pp. 165–186, https://doi.org/10.34752/2022-i280.

Plėta et al. 2020 – Plėta, T., Tvaronavičienė, M., Della Casa, S. and Agafonov, K. 2020. Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases. *Insights into Regional Development* 2(3), pp. 703–715, https://doi.org/10.9770/ird.2020.2.3(7).

Pshemyska, A. 2024. Ukrenergo's facilities are protected by 85 per cent – Shmyhal. [Online:] https://www.dw.com/uk/obekti-ukrenergo-zahiseno-na-85-vidsotkiv-smigal/a-70178375 [Accessed: 2025-12-08].

Pyshkin, S. 2024. Shmyhal on the protection of energy facilities: There are three levels of fortifications, one of them is experimental (*Shmyhal' pro zakhyst enerhoob'yektiv: ye try rivni fortyfikatsiy, odyn iz nykh eksperymental'nyy*). [Online:] https://www.rbc.ua/rus/news/shmigal-zahist-energoob-ektiv-e-tri-rivni-1724751478.html [Accessed: 2025-12-08] (*in Ukrainian*).

Qudus, L. 2025. Resilient systems: Building secure cyber-physical infrastructure for critical industries against emerging threats. *International Journal of Research Publication and Reviews* 6(1), pp. 3330–3346, https://doi.org/10.55248/gengpi.6.0125.0514.

Resolution of the Cabinet of Ministers of Ukraine No. 518 "On Approval of the General Requirements for Cyber Defence of Critical Infrastructure Facilities" 2019. [Online:] https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text [Accessed: 2025-12-08] (*in Ukrainian*).

Shchuka, V. 2025. The use of artificial intelligence for information campaigns in wartime: Visual tools for countering disinformation. *Technologies and Engineering* 26(2), pp. 89–98, https://doi.org/10.30857/2786-5371.2025.2.8.

Skochko et al. 2024 – Skochko, V.I., Solonnikov, V.H., Pohosov, O.H., Haba, K.O., Kulinko, Y.O. and Koziachyna, B.I. 2024. Minimization of Heat Losses in District Heating Networks by Optimizing their

Configuration. *Problems of the Regional Energetics* 3, pp. 182–195, https://doi.org/10.52254/1857-0070.2024.3-63.15.

Soldatos et al. 2020 – Soldatos, J., Philpot, J. and Giunta, G. 2020. Cyber-physical threat intelligence for critical infrastructures security: A guide to integrated cyber-physical protection of modern critical infrastructures. *Norwell: Now Publishers*, https://doi.org/10.1561/9781680836875.

Stoliarov, O. 2024. Efficient electricity generation forecasting from solar power plants using technology: Integration, benefits and prospects. *Bulletin of Cherkasy State Technological University* 29(1), pp. 73–85, https://doi.org/10.62660/bcstu/1.2024.73.

Tabansky, L. 2025. Critical infrastructure protection policy: The Israeli experience. *Journal of Information Warfare* 12(3). [Online:] https://www.jinfowar.com/journal/volume-12-issue-3/critical-infrastructure-protection-policy-israeli-experience [Accessed: 2025-12-08].

Telbayeva et al. 2023 – Telbayeva, S., Nurmaganbetova, G., Avdeyev, L., Kaverin, V., Issenov, S., Janiszewski, D., Smagulova, K. and Nurmagambetova, G. 2024. Development of mathematical models of power consumption at coal plants. *Eastern-European Journal of Enterprise Technologies* 5(8(131)), pp. 22–32, https://doi.org/10.15587/1729-4061.2024.313932.

The U.S.-Israel Cybersecurity 2021. [Online:] https://aipacorg.app.box.com/s/7bdvf60hrmjpyywa4th0vgh d23tetxf7 [Accessed: 2025-12-08].

Topor, S. 2023. The trench electronic warfare – A new threat to critical infrastructures. *Romanian Cyber Security Journal* 2(5), pp. 3–11, https://doi.org/10.54851/v5i2y202301.

U.S. Agency for International Development 2025. Reports. [Online:] https://energysecurityua.org/reports/.

United Nations 2024. Attacks on Ukraine's Energy Infrastructure: Harm to the Civilian Population. [Online:] https://ukraine.ohchr.org/sites/default/files/2024-09/ENG%20Attacks%20on%20Ukraine%E2%80%99s%20Energy%20Infrastructure-%20%20Harm%20to%20the%20Civilian%20Population.pdf [Accessed: 2025-12-08].

United Nations Development Programme 2023. Ukraine Energy Damage Assessment. [Online:] https://www.undp.org/ukraine/publications/ukraine-energy-damage-assessment [Accessed: 2025-12-08].

Voitenko, V. and Polishchuk, R. 2025. Decentralised generation and its role in enhancing the resilience of energy islands and critical infrastructure: Current trends and prospects. *Technologies and Engineering* 26(2), pp. 11–26, https://doi.org/10.30857/2786-5371.2025.2.1.

Volkov et al. 2023 – Volkov, A., Brechka, M., Stadnichenko, V., Yaroshchuk, V. and Cherkashyn, S. 2023. The protection of critical infrastructure facilities from air strikes due to compatible use of various forces and means. *Machinery & Energetics* 14(4), pp. 23–32, https://doi.org/10.31548/machinery/4.2023.23.

Wisniewski et al. 2022 – Wisniewski, M., Gladysz, B., Ejsmont, K., Wodecki, A. and Van Erp, T. 2022. Industry 4.0 solutions impacts on critical infrastructure safety and protection – A systematic literature review. *IEEE Access* 10, pp. 82716–82735, https://doi.org/10.1109/ACCESS.2022.3195337.

Yu et al. 2021 – Yu, K., Tan, L., Mumtaz, S., Al-Rubaye, S., Al-Dulaimi, A., Bashir, A.K. and Khan, F.A. 2021. Securing critical infrastructures: Deep-learning-based threat detection in IIoT. *IEEE Communications Magazine* 59(10), pp. 76–82, https://doi.org/10.1109/MCOM.101.2001126.

Zhang, X. and Kusrini, K. 2021. Autonomous long-range drone detection system for critical infrastructure safety. *Multimedia Tools and Applications* 80(15), pp. 23723–23743, https://doi.org/10.1007/s11042-020-10231-x.

Zmysłowski et al. 2023 – Zmysłowski, D., Skokowski, P. and Kelner, J.M. 2023. Anti-drone sensors, effectors, and systems – a concise overview. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation* 17(2), pp. 455–461, https://doi.org/10.12716/1001.17.02.23.

Oleh Semenenko, Svitlana Zakharova, Andrii Gorlichenko, Oleksandr Signaievskyi, Oleksandr Fedchenko

Innowacyjne technologie ochrony obiektów energetycznych infrastruktury krytycznej przed działaniami wojennymi

Streszczenie

Celem niniejszego badania była kompleksowa analiza technologii ochrony obiektów energetycznych infrastruktury krytycznej w Ukrainie w warunkach wojennych. Metodologia badań łączyła jakościowe i ilościowe metody gromadzenia i analizy danych, w tym analizę porównawczą, badanie praktycznych doświadczeń Ukrainy oraz standardy międzynarodowe, aby zapewnić kompleksowe zrozumienie ochrony obiektów energetycznych infrastruktury krytycznej. W wyniku badania zauważono, że w 2021 r. infrastruktura energetyczna Ukrainy miała moc 53,3 GW i wyprodukowała 158,4 mld kWh, ale po inwazji rosyjskiej w 2022 r. straciła dwie trzecie swojej mocy – do połowy 2024 r. wyniosła ona łącznie ~15,4 GW z powodu zajęcia Zaporoskiej Elektrowni Jądrowej i zniszczenia kluczowych obiektów. Ustalono, że nowoczesne technologie i środki ochrony obiektów energetycznych odegrały ważną rolę w zapewnieniu odporności systemu energetycznego na zagrożenia fizyczne i cybernetyczne, zwłaszcza w kontekście wojny hybrydowej. Zauważono również, że cyberbezpieczeństwo, wzmocnione systemami monitoringu zintegrowanymi ze sztuczną inteligencją, a także technologiami ochrony danych i segmentacji sieci, znacząco poprawiło bezpieczeństwo cyfrowych systemów sterowania, zapewniając odporność na wyrafinowane cyberataki. Nowoczesne technologie, a w szczególności druk 3D, umożliwiły szybką produkcję części zamiennych do sprzętu, a kompaktowe i łatwe w transporcie transformatory modułowe zapewniły szybkie przywracanie dostaw energii. Wyniki badania mogą zostać wykorzystane do opracowania i wdrożenia kompleksowych systemów ochrony obiektów energetycznych na ukraińskich obszarach przyfrontowych, przy uwzględnieniu realnych warunków prowadzenia działań wojennych i ograniczonych zasobów.

Słowa kluczowe: zagrożenia hybrydowe, bezzałogowe statki powietrzne, szybkie odzyskiwanie, standardy międzynarodowe, cyberataki, bariery fizyczne