JOURNAL OF MODERN SCIENCE

2/66/2026

www.jomswsge.com

DOI: 10.13166/jms/224789

Pavlo Fris
Vasyl Stefanyk Precarpathian National University, Ukraine
ORCID iD: 0000-0003-4979-051X

Tomasz Kośmider
WSB University Merito Poznan, Poland
ORCID iD: 0000-0003-2129-3642

Igor Kozych
Vasyl Stefanyk Precarpathian National University, Ukraine
ORCID iD: 0000-0002-8746-1154

Yuriy Mykytyn
Vasyl Stefanyk Precarpathian National University, Ukraine
ORCID iD: 0000-0002-9354-3586

THE LEGAL AND ADMINISTRATIVE DIMENSION OF CRITICAL INFRASTRUCTURE PROTECTION IN UKRAINE UNDER CONDITIONS OF FULL-SCALE WAR

Abstract

This article examines how Ukraine's legal and administrative system for the protection of critical infrastructure has been transformed by the full-scale Russian aggression that began on 24 February 2022, and the extent to which that system corresponds to the contemporary European paradigm of critical-entity resilience. Adopting a doctrinal (formal-dogmatic) approach combined with hermeneutic, systematic-analytical and comparative methods, the study analyses strategic documents, primary legislation, by-laws and institutional practice in force between 2014 and January 2026. The findings are presented in four analytical strands: the regulatory framework; the multi-level institutional architecture and the distribution of competences; the criteria for classifying and categorising facilities; and the financing of protection. These are complemented by an empirical assessment of the scale of war-related damage and of the adaptive measures introduced during martial law. The study finds that Ukraine's system is migrating from an object-protection model towards a broader model of state and essential-service resilience, but that its effectiveness is constrained by regulatory fragmentation, an emergency-driven manual mode of governance, resource asymmetries between operators and the still-incomplete harmonisation with the EU acquis, in particular Directive (EU) 2022/2557 (the CER Directive) and Directive (EU) 2022/2555 (NIS2). The article identifies the systemic gaps that remain and sets out directions for reform and further research.

Keywords: *protection of critical infrastructure; resilience of critical-entity; national security; martial law; multi-level governance; classification of critical infrastructure; EU harmonisation; CER Directive; NIS2*

1. Introduction

The security of a modern state depends to a large extent on the ability of its institutions to anticipate, absorb and neutralise negative impacts, and to build adequate response capacity (Shumilo et al., 2021). Designing security policy requires accounting for the most likely scenarios of crisis, including not only hybrid or asymmetric pressure but full-scale armed aggression; a key challenge in that setting is safeguarding critical infrastructure and coordinating military and non-military needs (Kośmider, 2021; Yefimenko et al., 2023). Ukraine, which has been at war since 24 February 2022, offers an unusually instructive case of how a legal and administrative system for protecting strategically important facilities behaves when it is placed under sustained, deliberate attack.

The reliable functioning of facilities that are strategically important for the economy, society and the state has become acutely relevant for Ukraine. Between 24 February 2022 and the beginning of 2026 the aggressor destroyed or damaged more than 700 critical-infrastructure objects, concentrating its strikes on the energy system; cumulative losses in the energy sector alone exceeded USD 56 billion by January 2026. Such pressure tests not merely the physical robustness of facilities but the coherence of the legal regime, the clarity of institutional competences and the capacity of the state to finance protection and recovery. These are precisely the questions that legal scholarship, security studies and public administration must address jointly.

Existing Ukrainian literature on critical infrastructure is substantial but uneven. Conceptual and definitional questions have been developed by Yermenchuk (2018) and by Biriukov, Kondratov, Nasvit and Sukhodolia (2015) in the influential *Green Paper* on critical-infrastructure protection; administrative-law mechanisms were analysed in depth by Krykun (2021); financing has been examined by Klymenko, Pavliuk and Savostianenko (2021) and by Radchenko, Tulush and Leontovych (2023); and the wartime functioning of civil protection has been studied by Mykytyn, Kośmider and Snopek (2023) and Vhpiliarevych, Tocicka and Szafrańska (2023). What is still largely missing is an integrated legal-administrative account that treats the 2021 framework Law, its wartime amendments and the new European resilience paradigm as a single, evolving system. This article seeks to fill that gap.

The **research problem** addressed here is how Ukraine's legal and administrative system for the protection of critical infrastructure has been transformed by the full-scale aggression, and to what degree it aligns with the contemporary paradigm of critical-infrastructure resilience embodied in EU law. The article does not aim to describe the legislation exhaustively; rather, it interrogates the coherence of the regulatory system, the allocation of institutional responsibility, the classification and financing mechanisms, and the gap between the law on the books and its implementation under war.

2. Theoretical and conceptual framework

Because the article assesses Ukraine's system against an evolving paradigm, it is necessary first to fix the key concepts and to distinguish the terms used in Ukrainian legislation from those used in EU law.

Infrastructure is conventionally understood as the set of interdependent structures, systems and services that provide the basis for the functioning of the economy and of social life (Yermenchuk, 2018). Infrastructure becomes **critical** where its disruption, degradation or destruction would cause the most serious negative consequences for the life of society, socio-economic development and national security. The term *critical* here is used not in the evaluative sense of *fault-finding* but in the sense of a threshold state beyond which danger and crisis materialise; *critical infrastructure* therefore denotes physical and virtual systems, objects and resources whose incapacitation or destruction would generate substantial threats to the state, its national security and the life and health of the population (Biriukov et al., 2015).

Critical infrastructure protection (CIP) has traditionally referred to the organisational, legal, engineering-technical and other measures aimed at the timely detection, prevention and neutralisation of threats to facilities, and at minimising and eliminating consequences when threats materialise. The contemporary literature, however, embeds CIP within the broader concept of **resilience** – the capacity of a system to withstand, absorb, recover from and adapt to adverse events while maintaining continuity of vital functions (Azarov et al., 2021). Resilience is commonly decomposed into four components: preparedness, mitigation, response and recovery. Whereas *security* seeks to reduce the probability or impact of attacks and disasters through physical and cyber defences, *resilience* presupposes that some disruptions will succeed and asks how quickly and how completely essential services can be restored.

This conceptual shift is mirrored in the vocabulary of EU law, which speaks of **critical entities** – the public or private operators that provide **essential services** – rather than of isolated assets. Related notions that structure the present analysis include **risk management** (the systematic identification, assessment and treatment of threats across the asset life-cycle), **business continuity** (the operator's ability to maintain or rapidly resume critical functions),

sectoral interdependencies (the cascading effects that a failure in one sector produces in others), and **public–private partnership (PPP)** as the governance principle that distributes protection duties between the state and operators of various forms of ownership.

A note on terminology is warranted, because the two legal orders are not perfectly aligned. Ukrainian law works with the umbrella term *critical infrastructure* (defined as the aggregate of *critical infrastructure objects*), with *critical infrastructure operators* as the responsible duty-bearers, and with *critical information infrastructure* for the cyber dimension. EU law, by contrast, centres on *critical entities* and *essential services* and treats the cyber layer separately under NIS2. Throughout this article, *object* and *facility* are used to render the Ukrainian object-centred terminology, *operator* for the Ukrainian duty-bearer, and *critical entity* / *essential service* only where EU law is being discussed. Maintaining this distinction is itself analytically significant, because the difference in vocabulary reflects the very paradigm shift the article examines.

3. Research methodology

3.1. Objectives

The **main objective** of the study is to assess the coherence and effectiveness of Ukraine's legal and administrative system for the protection of critical infrastructure and the degree of its alignment with the EU resilience paradigm under conditions of full-scale war. The **specific objectives** are: (I) to reconstruct the regulatory framework and trace its evolution; (II) to identify the institutional actors and to analyse the distribution of competences among them; (III) to evaluate the mechanisms for classifying and categorising facilities; (IV) to analyse the instruments financing protection and recovery; and (V) to assess the system's strengths, weaknesses and harmonisation with EU law.

3.2. Research questions

The study is guided by five interrelated research questions. It asks, first, which legal acts and strategic documents form the basis of critical infrastructure protection in Ukraine and how that basis has changed since 2014. It then

examines how competences are distributed among central and local authorities, infrastructure operators and the security and defence sector, and which criteria for classifying and categorising facilities have been adopted in Ukrainian law. A further question concerns the extent to which Ukrainian solutions are consistent with the development of EU law, and in particular with the CER Directive and the concept of critical-entity resilience. Finally, the study asks what regulatory and organisational gaps can be identified in the system as it currently operates. These questions structure the results reported in Section 4 and are returned to, in synthetic form, in the conclusions.

3.3. Hypothesis

The study tests the hypothesis that **Ukraine's critical-infrastructure protection system is evolving from an object-protection model towards a broader model of state and essential-service resilience, but that its effectiveness is limited by regulatory fragmentation, the conditions of war, a reliance on emergency and *manual* solutions, and the need for further harmonisation with EU standards.**

3.4. Scope of the research material and source-selection criteria

The temporal scope of the study runs from 2014 – the onset of Russian aggression, which reframed Ukrainian security policy – to January 2026, with the legal status of acts stated as of that date. The material analysed comprises four categories of source: (I) strategic documents (national-security, military-security and cyber-security strategies; the resilience concept; the National Plan for the Protection of Critical Infrastructure); (II) primary legislation (above all the 2021 framework Law *On Critical Infrastructure* and its 2022–2024 amendments, together with sectoral and security-sector statutes); (III) by-laws (Cabinet of Ministers resolutions and orders, and ministerial and agency acts on categorisation, security plans, cyber-protection and air-defence); and (IV) EU law and the relevant scholarly literature.

Acts were selected on the basis of their direct regulatory bearing on the protection, security or resilience of critical infrastructure, prioritising framework instruments and those amended or adopted during martial law; numerous purely technical sub-sectoral acts (of which there are several hundred)

were deliberately excluded, since enumerating them would not advance the analytical aim. The principal limitation of the study is characteristic of wartime research: a significant share of operational information – security passports, object protection plans, monitoring results and information concerning facilities of the first and second criticality categories – has been classified as restricted-access or, since the 2025 amendments to the Law *On State Secrets*, as a state secret. The analysis therefore relies on the publicly available legal and strategic record and on aggregate, officially reported data.

3.5. Methods and analytical procedure

The study combines four methods. The **formal-dogmatic method** is used to establish the content, structure and internal consistency of legal acts and to derive doctrinal definitions from statutory criteria. The **hermeneutic method** supports the interpretation of legal and strategic concepts – notably *protection*, *security* and *resilience* – and the reconstruction of legislative intent. The **systematic-analytical method** organises the regulatory material into analytical categories and exposes the relationships among them. The **comparative method** situates Ukrainian solutions against EU standards, in particular the transition from Directive 2008/114/EC to the CER and NIS2 Directives. Procedurally, the material was examined under the following categories: definitions and terminology; system actors and the distribution of competences; classification and categorisation of facilities; financing mechanisms; cyber-security; the empirical impact of aggression and the adaptive wartime response; and harmonisation with EU law. The results reported in Section 4 follow this procedure.

4. Results

4.1. The regulatory framework and its evolution

Before 2021, Ukrainian law did not use the term *critical infrastructure* as an organising category. Protection was addressed sector by sector through the regimes for *enterprises of strategic importance*, *potentially dangerous objects*, *high-hazard objects* and *especially important objects of the power industry*, oriented above all towards preventing technogenic accidents and protecting civilians from their consequences rather than towards deliberate hostile action (Krykun, 2021). The hybrid war launched in 2014 – including the seizure of gas-transmission facilities, the capture of energy assets in occupied Crimea and armed incidents near the Zaporizhzhia nuclear power plant – made plain that this fragmented, accident-centred regime was inadequate to the threat.

The strategic response developed in stages. The National Security Strategy of 2015 was, paradoxically, more explicit on critical infrastructure than its 2020 successor: it identified the insufficient physical protection of infrastructure and ineffective security management as distinct threats and devoted a dedicated section to comprehensively improving the legal basis, creating a state management system, and developing public–private partnership and information-sharing. The 2020 Strategy, built on the concept of comprehensive security, paid markedly less attention to the subject, confining itself to noting the growing threats and the task of building *an effective system of security and resilience of critical infrastructure* based on a clear allocation of responsibility and on public–private partnership. Successive doctrinal documents were inconsistent: the 2021 Military Security Strategy omitted critical infrastructure almost entirely, while the 2021 Cyber Security Strategy and the Strategic Defence Bulletin reintroduced and systematised the security-sector actors responsible for it.

The central instrument is the **Law** *On Critical Infrastructure* of 16 November 2021, which entered into force on 16 December 2021 but came into effect only on 16 June 2022 – that is, after the full-scale invasion had begun. For the first time the Law defined the aim and tasks of state policy in the field, established the principles of the national protection system (unity of methodology, coordination, public–private partnership, protection of restricted-access information, and international cooperation), and set out the procedure and criteria for

designating facilities. Its adoption on the eve of the active phase of aggression, although its full institutional machinery lagged behind events, nonetheless gave the state a framework on which to build during the war. That framework was then repeatedly amended under fire – among others by Law No. 2158-IX of 24 March 2022 (clarifying the role of the Armed Forces), Law No. 3931-IX of 22 August 2024 (refining the powers of public authorities and the list of system actors), and the February 2025 amendments to the Law *On State Secrets* (reclassifying protection-related information for category I and II facilities). Table 1 summarises the principal instruments.

Table 1. *Principal Ukrainian legal and strategic instruments on critical infrastructure protection (as of January 2026)*

Instrument	Rank / act	Principal regulatory content
Concept of the State System for the Protection of Critical Infrastructure	CMU Order No. 1009-r, 06.12.2017	First conceptual document; directions, mechanisms and time-frames (short-, medium- and long-term) for comprehensive regulation and for building a state management system.
National Security Strategy	Presidential Decree No. 392/2020, 14.09.2020	Commits the state to an effective system of security and resilience of critical infrastructure, based on a clear allocation of responsibility and public–private partnership.
National Resilience System	Presidential Decree No. 479/2021, 27.09.2021	Provides for the safety and security of facilities, including continuity of food, water, energy, heat, transport and cyber-security.
Strategy for Ensuring State Security	Presidential Decree No. 56/2022, 16.02.2022	Identifies growing threats linked to temporary occupation, hybrid influence, deterioration of technical condition and unauthorised interference.
Law "On Critical Infrastructure"	Law No. 1882-IX, 16.11.2021 (in effect 16.06.2022)	Framework act: aim and tasks of policy; principles; criteria and procedure for designation; sectors; system actors; operators' duties.
Law "On National Security of Ukraine"	Law No. 2469-VIII, 21.06.2018	Counter-intelligence protection of facilities by the SBU; security and defence funding of at least 5% of GDP (at least 3% for the defence forces).
Law "On the Basic Principles of Cyber Security"	Law No. 2163-VIII, 05.10.2017	Cyber resilience and protection of the national information infrastructure, including critical information infrastructure.
Security-sector statutes	Laws on the SBU, National Police, Armed Forces, National Guard, National Resistance	Allocate guarding, counter-intelligence, air-defence and crisis-response functions among security and defence actors.
By-laws on designation and categorisation	CMU Resolution No. 1109, 09.10.2020; Resolutions Nos. 943 (2020), 151/NBU (2020)	Procedure for designating facilities and the categorisation methodology; critical information-infrastructure and banking-sector lists.
National Plan for the Protection, Security and Resilience of Critical Infrastructure	CMU Order No. 825-r, 19.09.2023	Coordination among system actors; monitoring; risk assessment; information-sharing; community-resilience programmes; international cooperation.

4.2. Institutional architecture and the distribution of competences

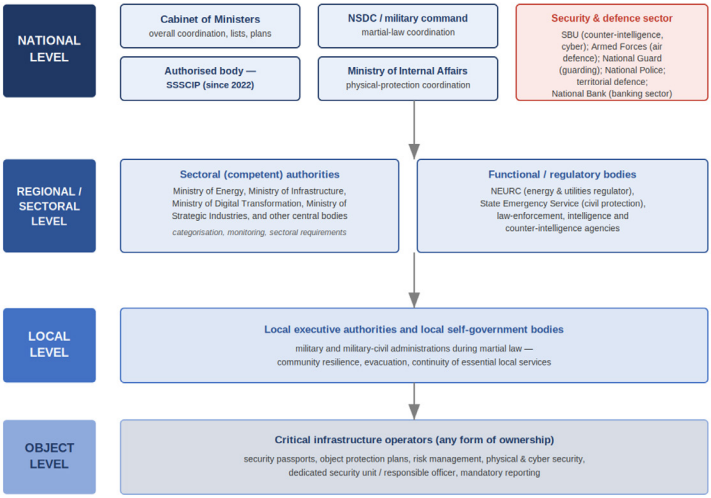
Under the Law, governance of the field is organised across four levels – national, regional/sectoral, local and object (see Figure 1). At the **national level**, the Cabinet of Ministers ensures the formation and implementation of policy and, in practice, performs the high-level coordinating function by approving the list of facilities requiring protection and their protection plans. A central executive body with special status acts as the **authorised body** for the national system. A decisive institutional fact – absent from much of the descriptive literature – is that, since 2022, this role has been assigned to the **State Service of Special Communications and Information Protection (SSSCIP)** for the duration of martial law and for twelve months thereafter. Locating the authorised body within the cyber-protection agency is significant: it ties the national coordination of physical protection to the institution responsible for information security, reflecting the convergence of physical and cyber threats.

Physical-protection coordination has been concentrated in the **Ministry of Internal Affairs**, a choice dictated by the fact that, apart from the General Staff of the Armed Forces, it is the only executive body commanding armed formations – the National Guard – able to guard and defend facilities. A coordinating vertical has thus emerged in which the Cabinet of Ministers approves lists and plans, the Ministry of Internal Affairs plans physical protection in peacetime and coordinates with the General Staff during martial law, and the General Staff develops protection and defence tasks for the period of martial law. The **National Security and Defence Council** retains monitoring and oversight functions. At the **regional and sectoral level**, competent (sectoral) authorities – the Ministry of Energy, the Ministry of Infrastructure, the Ministry of Strategic Industries, the Ministry of Digital Transformation and others – carry out categorisation, monitoring and the setting of sectoral requirements, while functional and regulatory bodies such as the energy and utilities regulator (NEURC) and the State Emergency Service perform specialised tasks. The **local level** is administered by local executive authorities and self-government bodies (replaced by military or military-civil administrations during martial law), and the **object level** rests with operators of any form of ownership. Table 2 sets out the principal actors and their functions.

Table 2. *Principal actors of the national critical-infrastructure protection system and their competences*

Actor	Principal competences
Cabinet of Ministers of Ukraine	Forms and implements policy; approves the list of facilities requiring protection and their protection plans; allocates forces and means; high-level coordination.
Authorised body — SSSCIP (since 2022)	Functional management of the national system; coordination of ministries and operators; methodology for assessing the level of protection; international cooperation.
Ministry of Internal Affairs	Coordinates physical protection; plans protection and the allocation of forces; commands the National Guard; prepares legislative proposals.
Security Service of Ukraine (SBU)	Counter-intelligence protection of facilities; protection of critical information infrastructure; cyber-incident response; coordination of counter-terrorism.
Armed Forces of Ukraine	Protection of military critical-infrastructure facilities; air-defence cover of important state facilities; tasks under the martial-law regime.
National Guard of Ukraine	Guarding of designated facilities (including nuclear installations and especially important objects); participation in eliminating the consequences of crisis situations.
National Police	Contractual protection of designated facilities; countering criminal encroachments, including in cyberspace.
State Emergency Service	Civil protection; protection of population and territories from emergencies; functions relating to high-hazard objects.
Sectoral (competent) authorities	Data collection and analysis; categorisation within their sectors; development and enforcement of protection norms; risk and threat assessment.
NEURC (energy & utilities regulator)	Designation in the financial-adjacent energy/utilities sphere; oversight of resilience, investment programmes and "green" transformation of energy operators.
National Bank of Ukraine	Determines and maintains the list of critical-infrastructure facilities in the banking system; sets cyber-protection requirements and independent-audit rules.

Figure 1. *Multi-level governance of critical infrastructure protection in Ukraine*



4.3. Classification and categorisation of facilities

Facilities are designated as critical on the basis of a set of statutory criteria reflecting their social, political, economic and environmental significance: the performance of functions ensuring vital national interests; the existence of challenges and threats; the vulnerability of facilities and the severity of possible consequences for public health, the social sphere, state sovereignty, the economy and natural resources; the scale of negative consequences and their duration; and the impact on interdependent sectors. On this basis the Law establishes four categories of criticality – (I) especially important objects of national importance; (II) vital objects of regional importance; (III) important objects of local importance; and (IV) necessary objects of local significance – with the volume of security powers and responsibility, and their distribution between the state and the owner, scaled to the category. The detailed procedure and methodology are set out in Cabinet of Ministers Resolution No. 1109 of 9 October 2020. The Law also enumerates seventeen sectors of essential functions and services, from governance and energy supply to transport, finance, defence, civil protection and research – a breadth that, as Section 5 shows, brings the Ukrainian taxonomy close to the EU's sectoral coverage.

4.4. Financing of protection and recovery

Protection is financed from several sources. The state budget funds the security and defence sector (at least 5% of GDP, of which at least 3% for the defence forces), the operation of the authorised body and dedicated state programmes; local budgets and operators' own investments supplement these. International technical and financial assistance – EU programmes, concessional loans and grants from international financial organisations – has become indispensable, as have special instruments: *military bonds* introduced in February 2022, *green bonds* under the 2022 Concept for the green-bond market, and dedicated funds such as the Energy Support Fund created by the Energy Community. For reconstruction, the Connecting Europe Facility – the EU's key instrument for financing transport, energy and digital infrastructure – is expected to play a central role (Balakin, 2021; Radchenko et al., 2023). The acquisition of EU candidate status has widened access to these channels, while the post-2022 *green* transformation, overseen by NEURC through net-billing and guarantees-of-origin

mechanisms, has begun to reorient financing towards distributed generation that reduces dependence on a few vulnerable trunk nodes.

4.5. The empirical impact of aggression

The scale of the deliberate targeting of critical infrastructure is the central empirical fact against which the system must be assessed. In the 2014–2022 period Ukraine lost control of roughly 90% of the coal mines in Donetsk and Luhansk oblasts and approximately 4 GW of generating capacity through occupation, together with the offshore assets of Chornomornaftogaz; direct physical damage exceeded USD 16 billion and indirect losses USD 40 billion, with damage in the infrastructure sector estimated at around USD 170 billion.

The full-scale invasion sharply escalated this pattern. By early 2026 more than 700 critical-infrastructure objects had been destroyed, with the energy system the priority target of repeated mass missile and drone strikes. The first wave of attacks created a capacity deficit of about 20%; by early 2023 the electricity sector's functionality had fallen by 61% and available capacity from roughly 36 GW to 13.9 GW, with about 10 GW – including 6 GW from the occupied Zaporizhzhia nuclear power plant – outside Ukrainian control. The mass strike of 15 November 2022, in which around 100 missiles were launched, was directed in part at the infrastructure of Ukrainian nuclear power plants. Since the start of the invasion the energy system has lost some 30 GW of capacity; in 2024 alone more than 9 GW of manoeuvrable generation (thermal and hydroelectric) was destroyed, with Tsentrenergo losing 100% of its capacity and private thermal operators such as DTEK sustaining damage to more than 80% of their equipment. As of January 2026 the energy sector was operating at 60–65% of its normal capacity and cumulative energy-sector losses exceeded USD 56 billion. Beyond energy, at least 18 airports and civil aerodromes, no fewer than 344 bridges and crossings and more than 25,000 km of roads had been damaged; in January 2026 alone the aggressor launched more than 6,000 attack drones, some 5,500 guided aerial bombs and 158 missiles of various classes, so that any aggregate figure is provisional and rises with each strike.

These physical attacks are compounded by a sustained cyber campaign whose principal vectors include attacks on the banking system and payment services, attempts to destabilise grid-management systems, intrusions into

government services and state registries, and disinformation operations aimed at undermining public trust. The targeting of nuclear facilities – strikes affecting the plants at Khmelnytskyi, Rivne and Pivdennoukrainsk, and the continuing occupation of Europe's largest plant at Zaporizhzhia – illustrates that the threat to Ukrainian critical infrastructure is also a threat of trans-boundary catastrophe. This empirical record explains why the legal regime has been driven so insistently towards resilience, redundancy and rapid recovery rather than static, perimeter-based protection.

4.6. Adaptive measures introduced during martial law

Wartime practice has generated a distinct body of operator obligations and state mechanisms. Operators must prepare and agree on a **security passport** for each facility, develop and implement an **object protection plan** covering physical protection, threat counteraction, information security and cyber-security, ensure **categorisation** under the methodology, and – for category I facilities – satisfy enhanced **risk-management** requirements, including annual reporting. They must establish engineering-technical protection systems, test them half-yearly, comply with the General Cyber-Protection Requirements (updated in November 2025), and designate a dedicated security unit or responsible officer. Article 21 of the Law has effectively introduced elements of *militarisation* of operators: at the most important facilities civilian guards are replaced wholly or partly by National Guard units, a military access regime is imposed, and engineering defences are erected; operators must also create conditions for the work of the military, the SBU and law-enforcement and intelligence bodies on their premises.

The state has supplemented these duties with new instruments. By NSDC decision of 17 October 2023 the Cabinet of Ministers was tasked with urgent engineering and physical protection of energy facilities, the creation of equipment reserves and back-up control points, and population-warning arrangements. Cabinet Resolution No. 1506 of 19 November 2025 launched an experimental scheme allowing enterprises, irrespective of ownership, to form **air-defence groups** around their facilities, acting under military command within the integrated air-defence system and the digital command network, with operators entitled to acquire air-defence assets under agreed procedures.

A simplified construction regime for protective structures – permitting work to begin without urban-planning conditions and allowing expert review to run in parallel with construction – has accelerated the hardening and reconstruction of facilities, in line with the Strategy for the Development of the Fund of Protective Structures to 2034 and its principle that *protective structures are needed by everyone*. Finally, early-warning and monitoring systems increasingly integrate artificial intelligence and machine learning to automate the collection and analysis of large data volumes and to identify anomalous patterns indicative of emerging threats.

5. Discussion

5.1. Strengths and weaknesses of the Ukrainian system

The principal strength of the Ukrainian system is its demonstrated **adaptability**. A framework Law that came into effect after the invasion had begun was nonetheless serviceable, and the legislator has shown an unusual capacity to amend it under fire – clarifying military competences, reclassifying sensitive information, and authorising novel arrangements such as enterprise air-defence groups. The system has converted the protection of operators from a general commercial obligation into a strategic national-security priority, and it has begun to internalise the resilience paradigm: the statutory definition of *security of critical infrastructure* now expressly embraces functionality, continuity, recoverability, integrity and resilience, mapping onto the four-component model of preparedness, mitigation, response and recovery.

The weaknesses are equally clear. The regime remains **fragmented**: it is layered over older, accident-centred sectoral statutes that were never designed for deliberate hostile action, and – outside the nuclear sector – sectoral energy law still does not require a proper system of physical protection and defence, treating protection largely as a commercial relationship between operators and departmental guards. Governance has acquired a strong **emergency,** *manual* **character**: much of the wartime architecture rests on experimental schemes, temporary regimes and ad hoc NSDC decisions rather than on stable, codified rules. The concentration of authority – the authorised body in the SSSCIP,

physical coordination in the Ministry of Internal Affairs, and operational coordination in the General Staff – brings coherence but also rigidity, and a risk that bureaucratic inertia in large hierarchical structures will impede the rapid decision-making that active hostilities demand.

5.2. Implementation challenges and oversight

Three implementation challenges stand out. First, **coordination among agencies** is still imperfectly codified: the division of competence among the Cabinet of Ministers, the NSDC, the Ministry of Internal Affairs, the General Staff and the sectoral authorities requires further detailing to avoid conflicts of competence between civilian sectoral bodies and the security and defence sector, particularly in zones where the state cannot fully exercise its powers. Second, there is a pronounced **resource asymmetry** between powerful state corporations and smaller local operators whose capacity to meet demanding physical – and cyber-protection requirements is limited; unless state policy moves from the imposition of duties under Article 21 towards a service-and-support model using the public–private-partnership instruments of Article 25, the formal obligations risk outrunning real capability. Third, the **dual subordination** created by the requirement that operators establish a security unit answerable in substance to the state introduces an *internal state agent* into private enterprises, with attendant questions about accountability and the allocation of liability for damage.

These tensions are sharpened by the **secrecy–accountability trade-off**. The reclassification of protection-related information for category I and II facilities as a state secret is justified by the need to deny the aggressor knowledge of vulnerabilities, but it narrows the scope for parliamentary, audit and public oversight. The Law's own safeguards – annual audit of the authorised body and a triennial comprehensive assessment by the Accounting Chamber against international standards, parliamentary review of reports, and public access to the non-classified part of resilience reports – must therefore be calibrated so that secrecy does not become a shield against the detection of systemic mismanagement or the misuse of reconstruction funds. Strengthening independent external audit while widening the public portion of resilience reporting would reinforce both trust and the integrity of budget spending.

5.3. Comparative perspective and harmonisation with EU law

The concept of critical-infrastructure protection originated in the United States with Presidential Decision Directive 63 (1996) and was reinforced by the USA PATRIOT Act, and it spread thereafter to Germany, the United Kingdom, the Netherlands, the Czech Republic, Poland, Israel and others, each delimiting broadly similar sectors – energy, transport, telecommunications, finance, water, food, health and emergency services – with national variations (Yermenchuk, 2018; Biriukov et al., 2015). The most consequential comparator for Ukraine, however, is the European Union, whose own approach has recently undergone exactly the paradigm shift this article describes.

Until 2022 the EU framework was Council Directive 2008/114/EC, which provided a procedure for designating European critical infrastructure but was confined to the energy and transport sectors and focused exclusively on the protection of individual assets. Its 2019 evaluation found that, given the interconnected and cross-border nature of modern operations, asset-by-asset protection could not prevent disruption. The response was a decisive move from protection of assets to resilience of entities. **Directive (EU) 2022/2557** of 14 December 2022 – the Critical Entities Resilience (CER) Directive – repeals Directive 2008/114/EC and requires Member States to identify, supervise and support critical entities across eleven sectors and to ensure that those entities can prevent, resist, mitigate and recover from incidents; its companion, **Directive (EU) 2022/2555** (NIS2), establishes a high common level of cyber-security for essential and important entities, repealing Directive 2016/1148. Together they reframe the field around essential services, resilience and the integration of physical and cyber dimensions. Table 3 compares the Ukrainian model with these EU instruments.

Table 3. *The Ukrainian model compared with the EU CER and NIS2 Directives*

Element	Ukraine (Law No. 1882-IX and related acts)	EU (Directive 2022/2557 CER; Directive 2022/2555 NIS2)
Central concept	"Critical infrastructure" and "objects"; "security" defined to include resilience.	"Critical entities" providing "essential services"; resilience as the organising concept (CER).
Paradigm	Migrating from object protection towards state and essential-service resilience.	Explicit shift from asset protection (2008/114/EC) to entity resilience (CER).
Sectoral coverage	Seventeen sectors of essential functions/services.	Eleven sectors under CER (energy, transport, banking, health, water, digital, public administration, space, food, etc.).
Cyber dimension	Critical information infrastructure regulated separately; SSSCIP as authorised body; cyber-protection requirements updated 2025.	NIS2 establishes cyber-security obligations for essential and important entities, closely coordinated with CER.
Operator duties	Security passport, protection plan, categorisation, risk management, dedicated security unit, reporting.	Resilience measures, risk assessment, incident notification, designated points of contact.
Governance	Four-level governance; authorised body plus sectoral and security-sector actors; emergency/martial-law overlay.	National resilience strategy, competent authority and single point of contact in each Member State.
Status / timeline	Framework in force since 2022; active wartime amendment; EU candidate harmonising with CER/NIS2.	Transposition due 17 Oct 2024; resilience strategies by 17 Jan 2026; critical entities identified by 17 July 2026.

On this comparison Ukraine's trajectory runs broadly parallel to the EU's. The breadth of its sectoral taxonomy, the statutory embrace of resilience, and the institutional integration of physical and cyber protection through the SSSCIP all point towards convergence with the CER and NIS2 logic, and Ukraine has expressly committed to developing its regulation on the basis of these directives. The remaining distance is not primarily conceptual but institutional and practical: the EU model presupposes stable peacetime administration – a national resilience strategy, a single point of contact, predictable identification and notification cycles – whereas Ukraine is operating an emergency overlay under continuous attack. Full harmonisation will require translating the wartime, partly experimental arrangements into durable, codified resilience institutions of the kind the CER Directive contemplates.

6. Conclusions

The analysis supports the study's hypothesis. Ukraine's system for the protection of critical infrastructure is indeed evolving from an object-protection model towards a model of state and essential-service resilience, but its effectiveness is constrained by regulatory fragmentation, the conditions of war, a reliance on emergency and *manual* solutions, and the still-incomplete harmonisation with EU standards. Answering the research questions in turn yields the following synthetic findings:

- The basis of protection has shifted from a pre-2014 patchwork of sectoral, accident-centred regimes to a framework anchored in the 2021 Law *On Critical Infrastructure*, surrounded by national-security, resilience and cyber strategies and an expanding body of wartime by-laws and amendments.
- Competences are distributed across a four-level governance system in which the Cabinet of Ministers coordinates at the top, the SSSCIP acts as authorised body, the Ministry of Internal Affairs coordinates physical protection through the National Guard, the General Staff leads under martial law, and sectoral and security-sector bodies discharge specialised functions – a structure that is coherent in design but insufficiently codified at its inter-agency seams.
- Facilities are designated on multi-factor criteria and sorted into four categories of criticality, with protection duties scaled to category, across seventeen sectors.
- Ukrainian solutions are broadly consistent with the direction of EU law and with the move from Directive 2008/114/EC to the CER and NIS2 Directives, though convergence remains a work in progress.
- The principal gaps are the persistence of an emergency, experimental mode of governance; the inadequate physical-protection requirements in non-nuclear sectoral law; the resource asymmetry among operators; the under-specified inter-agency coordination; and the tension between wartime secrecy and democratic oversight.

Several reform directions follow:

- the wartime, experimental arrangements – air-defence groups, simplified construction regimes, manual coordination – should be consolidated into stable, codified resilience institutions;
- state policy towards operators should move from the imposition of duties to a service-and-support model built on public–private partnership;
- sectoral statutes, especially in energy, should be brought into line with the resilience paradigm;
- inter-agency competences should be delineated more precisely, particularly between civilian sectoral bodies and the security and defence sector;
- the secrecy regime should be balanced by strengthened independent audit and wider public resilience reporting. Continued legislative harmonisation with the CER and NIS2 Directives should accompany Ukraine's EU accession process.

The study is subject to the limitations inherent in wartime legal research: a substantial part of the operational record is classified, and the empirical figures are provisional and change with each new strike. Future research should therefore pursue, as conditions permit, empirical and case-study work with infrastructure operators and emergency services; deeper sectoral analysis of interdependencies and cascading effects; and detailed doctrinal comparison of Ukraine's transposition pathway against the CER and NIS2 implementation experience of EU Member States. Ukraine's path to building critical-infrastructure protection is unusual in its adaptability; its long-term stability will depend on the state's ability to move from *manual* wartime management to durable, decentralised and adequately resourced mechanisms of resilience across all levels of the institutional vertical.

References

Azarov, S. I., Sydorenko, V. L., Yeremenko, S. A., Pruskyi, A. V., & Demkiv, A. M. (2021). Zakhyst krytychnoi infrastruktury v umovakh nadzvychainykh sytuatsii [Protection of critical infrastructure in emergency situations] (P. B. Volianskyi, Ed.). Kyiv.

Balakin, R. L. (2021). Connecting Europe Fund in the EU critical infrastructure joint financing system. Finance of Ukraine, (10), 61–80. https://doi.org/10.33763/finukr2021.10.061

Biriukov, D. S., Kondratov, S. I., Nasvit, O. I., & Sukhodolia, O. M. (2015). Zelena knyha z pytan zakhystu krytychnoi infrastruktury v Ukraini [Green paper on critical infrastructure protection in Ukraine]. National Institute for Strategic Studies.

Ivačík, R., & Andrassy, V. (2023). Insights into the development of the security concept. Entrepreneurship and Sustainability Issues, 10(4), 26–39. https://doi.org/10.9770/jesi.2023.10.4(2)

Klymenko, K. V., Pavliuk, K. V., & Savostianenko, M. V. (2021). Svitova praktyka finansuvannia zakhystu krytychnoi infrastruktury [World practice of financing critical infrastructure protection]. Naukovi Pratsi NDFI, (3), 58–82.

Kośmider, T. (2021). Determinants of the process of creating national security. Journal of Security and Sustainability Issues, 11, 287–299. https://doi.org/10.47459/jssi.2021.11.25

Krykun, V. V. (2021). Administratyvno-pravovyi mekhanizm zakhystu obiektiv krytychnoi infrastruktury v Ukraini [Administrative-legal mechanism for the protection of critical infrastructure facilities in Ukraine] [Doctoral dissertation, Kharkiv National University of Internal Affairs].

Mykytyn, Y., Kośmider, T., & Snopek, M. (2023). Civil protection services in Ukraine in emergency during the legal regime of martial law. Journal of Security and Sustainability Issues, 13, 239–250. https://doi.org/10.47459/jssi.2023.13.26

Radchenko, O., Tulush, L., & Leontovych, S. (2023). Financial instruments for ensuring national security: Experience of Ukraine in military conditions. Insights into Regional Development, 5(1), 10–25. https://doi.org/10.9770/IRD.2023.5.1(1)

Shumilo, O., Lytvyn, I., Shablystyi, V., Kornyakova, T., & Popovich, I. (2021). Legal mechanism to ensure national security in the field of use of natural resources. Entrepreneurship and Sustainability Issues, 8(3), 455–470. https://doi.org/10.9770/jesi.2021.8.3(29)

Vhpiliarevych, V., Tocicka, J. W., & Szafrańska, K. (2023). Civil protection and protection of critical infrastructure in Ukraine during the conditions of the martial state. Journal of Security and Sustainability Issues, 13, 265–272. https://doi.org/10.47459/jssi.2023.13.29

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

Yermenchuk, O. P. (2018). Zakhyst krytychnoi infrastruktury v Ukraini: rozvytok systemy [Protection of critical infrastructure in Ukraine: development of the system]. Dnipro.

Legal acts and EU directives

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. OJ L 345, 23.12.2008. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114

Decree of the President of Ukraine No. 392/2020 of 14 September 2020 *On the National Security Strategy of Ukraine*. https://www.president.gov.ua/documents/3922020-35037

Decree of the President of Ukraine No. 479/2021 of 27 September 2021 *On the Introduction of the National Resilience System*. https://www.president.gov.ua/documents/4792021-40181

Decree of the President of Ukraine No. 56/2022 of 16 February 2022 *On the Strategy for Ensuring State Security*. https://zakon.rada.gov.ua/laws/show/56/2022

Decree of the President of Ukraine No. 64/2022 of 24 February 2022 *On the Introduction of Martial Law in Ukraine*.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). OJ L 333, 27.12.2022, pp. 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER Directive). OJ L 333, 27.12.2022, pp. 164–198. https://eur-lex.europa.eu/eli/dir/2022/2557/oj

Law of Ukraine No. 1882-IX of 16 November 2021 *On Critical Infrastructure*. https://zakon.rada.gov.ua/laws/show/1882-20

Law of Ukraine No. 2469-VIII of 21 June 2018 *On National Security of Ukraine*. https://zakon.rada.gov.ua/laws/show/2469-19

Law of Ukraine No. 2163-VIII of 5 October 2017 *On the Basic Principles of Ensuring Cyber Security of Ukraine*. https://zakon.rada.gov.ua/laws/show/2163-19

Law of Ukraine No. 2229-XII of 25 March 1992 *On the Security Service of Ukraine*. https://zakon.rada.gov.ua/laws/show/2229-12

Law of Ukraine No. 580-VIII of 2 July 2015 *On the National Police*. https://zakon.rada.gov.ua/laws/show/580-19

Law of Ukraine No. 1934-XII of 6 December 1991 *On the Armed Forces of Ukraine*. https://zakon.rada.gov.ua/laws/show/1934-12

Law of Ukraine No. 876-VII of 13 March 2014 *On the National Guard of Ukraine*. https://zakon.rada.gov.ua/laws/show/876-18

Law of Ukraine No. 1702-IX of 16 July 2021 *On the Fundamentals of National Resistance*. https://zakon.rada.gov.ua/laws/show/1702-20

Law of Ukraine No. 3931-IX of 22 August 2024 on clarifying the powers of public authorities in the field of critical infrastructure protection. https://zakon.rada.gov.ua/laws/show/3931-20

Law of Ukraine No. 4236-IX of 12 February 2025 amending the Law *On State Secrets*. https://zakon.rada.gov.ua/laws/show/4236-20

Order of the Cabinet of Ministers of Ukraine No. 1009-r of 6 December 2017 *On Approval of the Concept of Creation of the State System for the Protection of Critical Infrastructure.* https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80

Order of the Cabinet of Ministers of Ukraine No. 825-r of 19 September 2023 *On the National Plan for the Protection, Security and Resilience of Critical Infrastructure.*

Resolution of the Cabinet of Ministers of Ukraine No. 1109 of 9 October 2020 *Some Issues of Critical Infrastructure Objects* (procedure for designation and methodology of categorisation). https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF

Resolution of the Cabinet of Ministers of Ukraine No. 943 of 9 October 2020 on the procedure for forming the list of critical information infrastructure objects. https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF

Resolution of the Cabinet of Ministers of Ukraine No. 1506 of 19 November 2025 on the experimental project for strengthening air defence by involving enterprises in forming air-defence groups.