*Corresponding Author's Email: gorgievskaa.teodora@gmail.com
Proceedings of The World Conference on Security Studies
Vol. 3 Issue. 1, 2026, pp. 01- 16
DOI: https://doi.org/10.33422/worldsecurityconf.v3i1.2074
Copyright © 2026 Author(s)
ISSN: 3030-1556 online

Hybrid Threats and Cascading Failures in Energy-Centric Critical Infrastructure

Teodora Gjorgjievska[1], Nikola Manev[2*], Neven Trajchevski[2], and Nenad Taneski[2]

[1]Institute of Security, Defence and Peace, Faculty of Philosophy, University of "Ss. Cyril and Methodius" Skopje, North Macedonia

[2]Military academy "General Mihailo Apostolski" – Skopje, Goce Delcev University, North Macedonia

Abstract

Modern societies depend on highly interconnected critical infrastructure systems, with the energy sector serving as a foundational enabler for virtually all other sectors. This interdependence increases vulnerability to hybrid threats that combine cyberattacks, physical sabotage, supply-chain disruptions, and information operations to exploit systemic weaknesses. Disruptions originating in the energy sector can propagate across dependent systems, producing cascading effects that compromise transportation, healthcare, water supply, communications, financial services, and public administration. Unlike studies that examine either hybrid threats or infrastructure interdependencies separately, this paper integrates both perspectives. Using a targeted narrative review, an explicitly defined qualitative screening rubric, and drawing on contemporary research in critical infrastructure resilience, interdependency analysis, and hybrid threat studies, the paper explores the mechanisms through which disruptions can spread across sectors and amplify their societal consequences. Furthermore, the national context of North Macedonia is examined, including the challenges associated with protecting interconnected infrastructure systems in an increasingly complex security environment. Empirical incidents illustrate different disruption pathways, while a phased national programme links roles, exercises, and continuity metrics to NIS2 and CER alignment. The paper concludes by outlining strategic recommendations aimed at strengthening resilience through cross-sector coordination, redundancy planning, interdependency-aware risk assessment, and integrated approaches to critical infrastructure protection.

Keywords: Interdependencies; Resilience; Risk Assessment; Energy Security; Disruptions

1. Introduction

Critical infrastructure systems constitute the backbone of contemporary societies. Their reliable operation is essential for economic activity, public safety, national security, and the delivery of vital services. Energy, transportation, information and communication technology (ICT), healthcare, finance, water supply, and public administration form highly interconnected systems whose functionality increasingly depends on the uninterrupted operation of other

sectors. Among these sectors, energy infrastructure occupies a uniquely central position (Pant et al., 2017). Electricity generation, transmission, and distribution enable the operation of virtually all modern services and technologies. Consequently, disruptions affecting energy systems frequently extend beyond the sector itself, triggering consequences throughout society. Historical incidents have demonstrated that failures within the energy sector can affect transportation networks, communication systems, financial services, healthcare facilities, water treatment plants, and emergency response capabilities (Zio and Sansavini, 2011; Ouyang, 2014).

At the same time, the security environment surrounding critical infrastructure has become increasingly complex. Hybrid threats have emerged as one of the most significant challenges facing modern states. These threats combine conventional and unconventional means, including cyber operations, physical sabotage, economic pressure, supply-chain manipulation, and information campaigns, to achieve strategic objectives while remaining below the threshold of conventional military conflict (Jungwirth et al., 2023).

The combination of increasing infrastructure interconnectivity and evolving hybrid threats creates conditions in which localized disruptions can rapidly evolve into broader systemic crises (Heracleous et al., 2017; Pant et al., 2017). Understanding these dynamics has become an essential requirement for policymakers, infrastructure operators, and national security institutions seeking to enhance resilience and ensure continuity of essential services (Ouyang, 2014).

This paper examines the relationship between hybrid threats and cascading failures in energy-centric critical infrastructure systems. In particular, the emphasis is placed on the mechanisms through which disruptions propagate across interconnected sectors and the implications of these processes for national resilience and critical infrastructure protection.

2. Methods

This study adopts a qualitative, analytical approach combining a targeted narrative review and synthesis of academic and institutional literature with conceptual framework development and contextual analysis of critical infrastructure interdependencies. The methodological approach is designed to examine the relationship between hybrid threat vectors, energy-centric critical infrastructure, cross-sector dependencies, and cascading failure mechanisms. Relevant academic literature and institutional sources addressing hybrid threats, critical infrastructure protection, infrastructure interdependencies, cascading failures, cyber-physical systems, resilience, and energy security were examined according to their relevance to the research problem. Particular attention was given to identifying recurring dependency relationships, disruption pathways, and resilience mechanisms that can explain how localized disruptions may propagate across interconnected infrastructure sectors.

The analysis is structured around three research questions:

- **RQ1:** How can hybrid threats targeting energy-centric critical infrastructure generate cascading failures across interconnected critical infrastructure sectors?
- **RQ2:** Which interdependencies and propagation pathways are particularly significant for the resilience of energy-centric critical infrastructure in North Macedonia?
- **RQ3:** How can interdependency-aware risk assessment and cyber-physical resilience approaches contribute to strengthening the protection of critical infrastructure against hybrid threats?

The research proceeds by first identifying the principal hybrid threat vectors affecting energy infrastructure, followed by an examination of the physical, cyber, geographic, organizational,

and logical interdependencies connecting energy infrastructure with other critical sectors. The analysis then considers the temporal characteristics of disruption propagation and identifies potential cascading pathways. Finally, these relationships are considered in the context of North Macedonia in order to derive implications for critical infrastructure resilience and protection.

The methodological approach is primarily analytical and conceptual, while the contextual assessment of North Macedonia provides a basis for applying the identified relationships within a national critical infrastructure context. The study focuses on sector-level dependencies and systemic cascading mechanisms that can inform resilience planning and future quantitative assessment.

With that said, the review is purposive: it integrates foundational interdependency studies, recent network-modeling research, publicly available incident investigations, and national and European policy sources. Inclusion is based on a source's relevance to an energy-origin disruption, an identifiable dependency or buffering mechanism, and implications for essential-service continuity. Peer-reviewed studies inform the conceptual mechanisms; institutional investigations anchor incident sequences; and national documents establish the policy context. It should be stressed that incident examples provide plausibility checks, not a representative sample or calibration dataset. The judgments are an interpretive synthesis of the cited literature and policy context.

2.1 Energy Infrastructure as a Strategic Target of Hybrid Threats

Energy systems have long been recognized as strategic assets whose disruption can generate consequences far beyond the immediate loss of electricity or fuel supply. Their central role within modern economies makes them attractive targets for both state and non-state actors seeking to create instability, exert political pressure, or undermine public confidence (Heracleous et al., 2017; Pant et al., 2017). The growing digitalization of energy infrastructure has introduced additional vulnerabilities. Modern energy systems increasingly rely on industrial control systems, supervisory control and data acquisition platforms, smart-grid technologies, and interconnected communication networks. While these developments improve efficiency and operational flexibility, they also expand the attack surface available to malicious actors (Gjorgjievska, 2025).

Cyberattacks against energy operators have become a recurring feature of the contemporary threat landscape (Kaspersky ICS CERT, 2025). Incidents affecting electricity distribution systems, fuel transportation networks, and industrial control environments have demonstrated the potential for cyber operations to disrupt essential services. When combined with physical attacks against infrastructure assets, such disruptions can significantly increase recovery times and amplify societal consequences. Hybrid threat actors may also employ disinformation campaigns designed to exploit infrastructure disruptions. False information concerning service outages, public safety, or government response measures can intensify societal stress, complicate crisis management efforts, and reduce trust in public institutions. As a result, the impact of a disruption is often determined not only by physical damage but also by the broader socio-technical environment in which it occurs (Buldyrev et al., 2010; Gong et al., 2023).

The strategic importance of energy infrastructure therefore extends beyond its technical functions. It represents a critical node within a broader ecosystem of interdependent systems whose stability underpins national resilience. As illustrated in Figure 1, hybrid threats may target energy infrastructure through multiple complementary pathways, while the resulting disruption may extend to other interconnected critical infrastructure sectors.

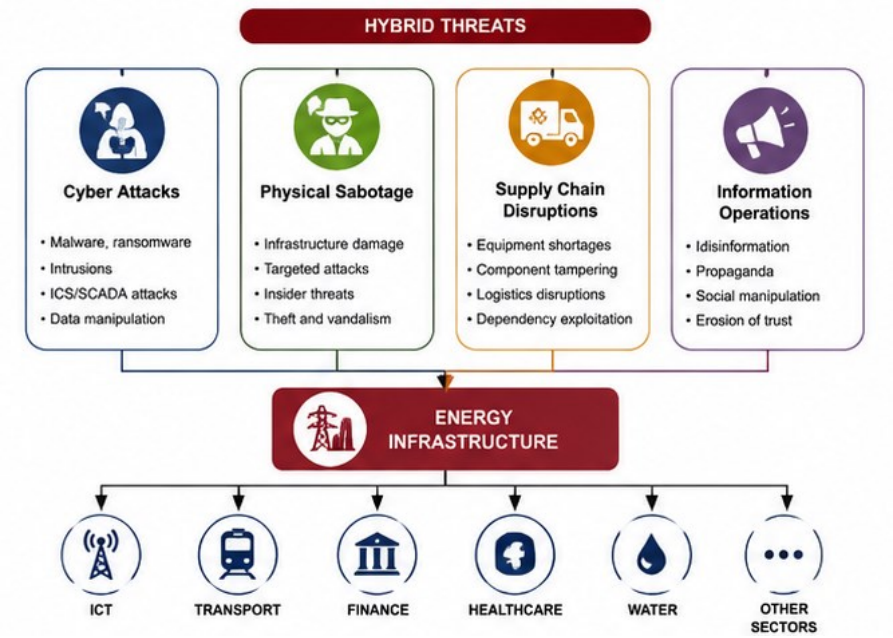


Figure 1. Hybrid Threat Pathways Targeting Energy Infrastructure

2.2 Critical Infrastructure Interdependencies and Failure Mechanisms

The increasing integration of critical infrastructure sectors has transformed the nature of infrastructure risk. Traditional approaches often focused on individual facilities or sectors in isolation. However, contemporary infrastructure systems operate as interconnected networks in which disruptions can propagate through multiple dependency pathways (Ouyang, 2014; Heracleous et al., 2017).

Interdependencies may take several forms. Physical interdependencies arise when one sector relies directly on the material outputs of another. Cyber interdependencies emerge through shared information systems, communication networks, and digital platforms. Geographic interdependencies occur when infrastructure assets are co-located or exposed to common hazards. Organizational and logical interdependencies are created through governance arrangements, operational procedures, and shared decision-making processes (Ouyang, 2014). These interconnections create conditions in which failures can spread from one sector to another. An interruption in electricity supply may affect telecommunications infrastructure, which in turn can disrupt emergency services, transportation management systems, and financial transactions. Similar patterns can emerge in reverse, where disruptions in communication networks impair the operation of energy infrastructure itself.

Cascading failures represent one of the most significant consequences of infrastructure interdependence. Rather than remaining localized, disruptions propagate through dependency chains, creating secondary and tertiary effects that may exceed the severity of the initial incident (Huang, 2014; Gong et al., 2023). The complexity of modern infrastructure systems often makes it difficult to anticipate the full extent of these effects, particularly when multiple sectors are affected simultaneously.

Recent network-science research extends single-layer representations toward multiplex and temporal models. Wang et al. (2024) review how multiplex networks represent different dependency types and address resilience evaluation, evolution, and control. Cimellaro et al. (2024) combine a modified inoperability input-output model with spatial multilayer networks and a temporal adjacency representation to examine the sequence and probability of failures.

Such approaches can distinguish dependency structure from time-dependent loss of function and recovery, which sector-level categories cannot resolve.

However, connectivity alone does not establish operational dependency: physical flows, control functions, backup autonomy, and restoration decisions require explicit modeling. Data scarcity, uncertain dependency strengths, and differences between topological and functional resilience constrain transfer to national planning. Hybrid-threat scenarios additionally require assumptions about simultaneous disruption and degraded coordination (Wang et al., 2024; Cimellaro et al., 2024).

In such circumstances, infrastructure operators and emergency management authorities may struggle to identify critical dependencies and prioritize response measures effectively. Figure 2 illustrates the principal mechanisms through which an initial disruption can propagate across interconnected infrastructure sectors, resulting in secondary and tertiary failures. Recognizing and understanding interdependencies therefore constitutes a fundamental prerequisite for effective resilience planning and critical infrastructure protection.

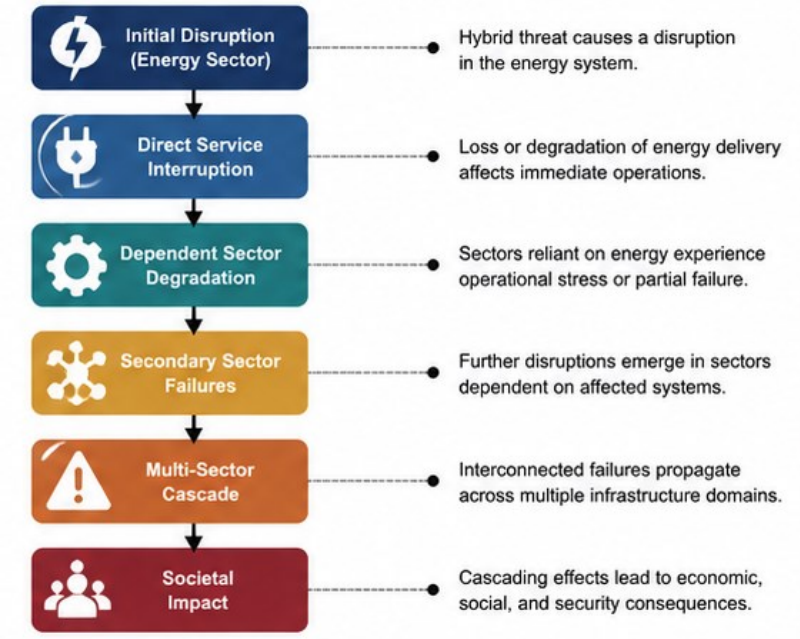


Figure 2. Cascading failure mechanisms in interdependent infrastructure
(Conceptual schematic: initiating disruption, direct service interruption, dependent-sector degradation, secondary failures, multi-sector cascade, and societal impact. The sequence is illustrative; feedback and parallel failures may occur.)

2.3 Speed of Cascading Failure Propagation

While cascading failures are often discussed in terms of their pathways and interdependencies, an equally important characteristic is the speed at which disruptions propagate across critical infrastructure sectors. Infrastructure systems exhibit considerable variation in their temporal response to disturbances, largely due to differences in operational processes, redundancy mechanisms, storage capacity, and dependence on continuous energy supply (Ouyang, 2014; Pant et al., 2017). Sectors such as energy and information and communication technology (ICT) can exhibit rapid failure dynamics. Power-dependent equipment without effective backup can stop within seconds or minutes; sector-wide loss of service depends on protection systems, alternative supply, and backup autonomy. Electricity interruptions may therefore immediately affect exposed telecommunications and control assets while other sites remain operational (Ouyang, 2014; Pant et al., 2017).

By contrast, other sectors demonstrate slower propagation dynamics. Water supply systems typically benefit from storage reservoirs and distribution buffers that temporarily maintain service during power interruptions. Similarly, food supply chains often possess inventory reserves and logistical flexibility that delay the manifestation of shortages, although prolonged disruptions eventually affect production, transportation, and distribution (Gong et al., 2023). Healthcare, transport, financial services, and public administration generally occupy an intermediate position, where backup power systems, operational redundancy, and emergency procedures provide limited resilience before cascading effects begin to accumulate (Heracleous et al., 2017; Gong et al., 2023).

These temporal differences have important implications for resilience planning. Rapidly propagating failures require immediate detection, automated response mechanisms, and highly coordinated incident management, whereas slower-moving cascades provide a valuable window for intervention before disruptions spread throughout the broader infrastructure network (Rinaldi et al., 2001). Consequently, understanding both the structural interdependencies between sectors and the characteristic speed of failure propagation is essential for prioritizing protective measures, designing effective contingency plans, and improving the resilience of energy-centric critical infrastructure systems (Ouyang, 2014; Weber et al., 2023).

Table 1 summarizes the indicative service-degradation times. The ordinal time-response categories express the urgency of intervention rather than numerical weights. The ranges describe sector-level planning assumptions; unprotected equipment may stop immediately, while functioning storage, batteries, generators, and manual procedures can delay material loss of service.

Table 1: Sector-Specific Response Characteristics and Ordinal Time-Response Categories

Sector	Typical Response / Propagation Time	Time-response category
Energy	Minutes – Hours	Very high
ICT	Minutes	Very high
Finance	Hours	High
Transport	Hours – Days	Moderate
Healthcare	Hours – Days	Moderate
Water	Hours – Days	Moderate
Food supply	Days	Very low
Public Administration	Hours – Days	Moderate

(Source: Authors' qualitative synthesis of Rinaldi et al. (2001), Ouyang (2014), Heracleous et al. (2017), and Gong et al. (2023)

3. Illustrative Cascading Failure Pathways in Energy-Centric Systems

Owing to the central role of electricity in supporting virtually all critical services, failures affecting energy infrastructure often initiate a sequence of cascading disruptions whose consequences unfold over different temporal and operational scales (Ouyang, 2014; Pant et al., 2017). However, actual propagation pathways depend on national infrastructure architecture, redundancy measures, and the nature of the initiating hybrid threat. The initial stage of a cascade typically involves direct impacts on electricity generation, transmission, or distribution systems. Such disruptions may result from cyberattacks targeting industrial control systems, physical sabotage of substations or transmission assets, supply-chain manipulation, or combinations of these actions characteristic of hybrid threats. Because modern energy infrastructure is closely integrated with digital monitoring and control platforms, cyber and physical attacks can reinforce one another, increasing both the severity of the initial disruption and the complexity of recovery (Gjorgjievska, 2025; Kaspersky ICS CERT, 2025).

Empirical incidents illustrate different initiating mechanisms and time scales. On 23 December 2015, coordinated cyberattacks against three Ukrainian electricity distribution companies interrupted supply to approximately 225,000 customers; the attacks were executed within 30 minutes of one another and outages lasted 1–6 hours (U.S. Department of Energy and U.S. Department of Homeland Security, 2018). CISA, FBI, and NSA (2022) also document the 2016 intrusion into a Ukrainian transmission company and deployment of grid-specific CrashOverride malware. These cases demonstrate a cyber-to-physical pathway and rapid interruption of electricity service.

As Table 1 goes to show, within minutes, failures can propagate to the ICT sector, where unprotected assets rely on uninterrupted electrical power to sustain telecommunications networks, internet connectivity, cloud services, and operational technology. Although backup power systems can temporarily maintain functionality, extended outages progressively reduce communication capabilities, limiting situational awareness and coordination among infrastructure operators and emergency services (Noebels, 2022). As communication capabilities deteriorate, secondary disruptions begin to emerge across dependent sectors (Srinivasan & Ni, 2023; Olorunlana & Mohammed, 2025). Transportation systems experience interruptions to railway signaling, traffic management, airport operations, fuel distribution, and logistics networks. At the same time, financial institutions may encounter degraded electronic payment systems, interruptions to banking services, and reduced availability of digital transactions. These disruptions compound the operational challenges faced by emergency responders and infrastructure operators attempting to restore essential services.

If energy shortages persist, cascading effects become increasingly widespread. Healthcare facilities may continue operating using emergency generators, yet prolonged disruptions can affect medical equipment, pharmaceutical supply chains, digital patient records, and emergency response capacity. Water supply and wastewater treatment systems face similar challenges, as pumping stations and treatment facilities require continuous electrical power. Extended interruptions therefore increase the risk of water shortages, sanitation failures, and secondary public health consequences (Heracleous et al., 2017; Gong et al., 2023).

Over longer time horizons, disruptions propagate beyond technical infrastructure into the broader socio-economic environment. Food production, refrigeration, distribution, and retail supply chains become increasingly constrained by transportation difficulties and limited energy availability. Public administration may experience reduced operational capacity as communication systems, digital government services, and emergency coordination platforms become unavailable.

Texas in February 2021 illustrates reciprocal gas–electricity dependencies under a natural hazard rather than a demonstrated hybrid attack. Fuel shortages and freezing impaired generation; electricity loss also disrupted gas-production and supply facilities, reinforcing supply constraints. FERC (2021) reports that some power outages lasted up to four days. The pathway shows how a rapidly developing power imbalance can become a prolonged service-continuity crisis when fuel supply and restoration are interdependent. It supports the need to test backup endurance and fuel access, without assigning the same delay to every dependent sector. Simultaneously, however, hybrid threat actors may exploit existing crisis through coordinated disinformation campaigns intended to amplify uncertainty, erode confidence in public institutions, and complicate crisis management efforts.

These cascading pathways illustrate that the overall impact of an energy-sector disruption is determined not solely by the magnitude of the initial event, but by the interaction between infrastructure interdependencies, temporal propagation dynamics, and the effectiveness of response measures. Consequently, resilience planning should focus not only on preventing

disruptions within individual sectors but also on identifying critical dependency chains capable of amplifying localized failures into systemic crises.

The September 2022 Nord Stream damage illustrates physical disruption of cross-border gas infrastructure and the need to distinguish asset damage from an observed electricity cascade (Council of the European Union, 2022). Nord Stream 1 deliveries had already stopped before the damage, so the incident should not be presented as causing an immediate new loss of those flows (Danish Energy Agency, 2022).

Regional evidence reinforces the relevance of interconnected operations. The 21 June 2024 South-East European disturbance affected Albania, Bosnia and Herzegovina, Montenegro, and Croatia; ENTSO-E (2025) identified vegetation-related initial faults, limited regional observability, and insufficient measures to prevent voltage collapse. More directly, the 18 May 2025 blackout in North Macedonia was attributed to operation above the 420 kV voltage limit and consequent tripping of all 400/110 kV transformers, separating the two voltage networks (ENTSO-E, 2026). These investigations document electrical failure mechanisms, not hostile attribution or quantified cross-sector impacts. They show why national resilience planning must include regional visibility, coordinated voltage control, and restoration arrangements alongside hybrid-threat preparedness.

Figure 3 provides a conceptual representation of the cascading failure pathways described in this section. It illustrates how hybrid threats may initiate a disruption in energy infrastructure, how this disruption can affect interconnected critical infrastructure sectors, and how secondary and tertiary effects may develop as the disruption propagates through existing interdependencies. The figure therefore summarizes the relationship between the initiating disruption, cross-sector propagation, and the broader systemic consequences discussed above.

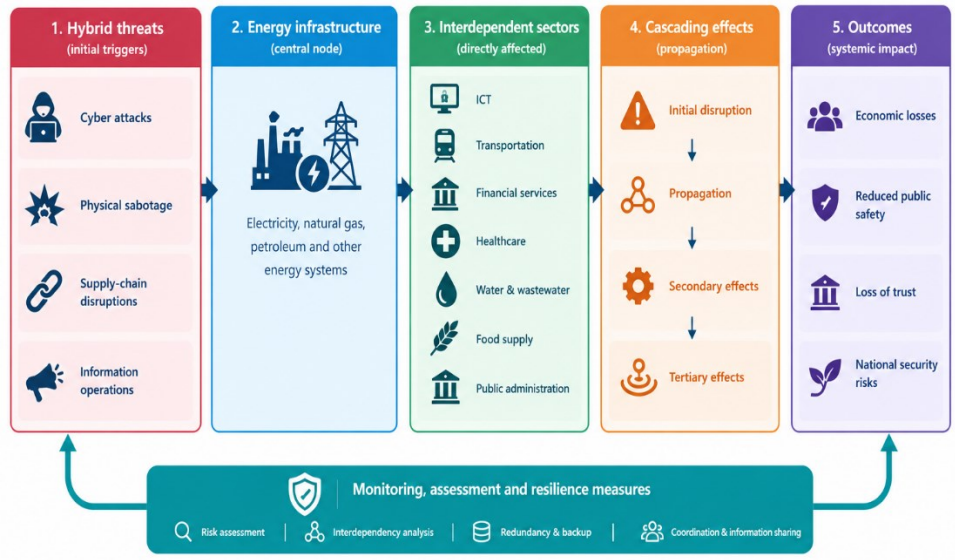


Figure 3. Critical infrastructure interdependency framework
(Note: Columns are analytical stages, not a fixed chronology)

3.1 National-Level Dependency Mapping for North Macedonia

To provide an analytical application of the cascading failure framework, the study considers the principal dependencies between energy infrastructure and selected critical infrastructure sectors in North Macedonia. The selection of sectors is supported by the National Security Strategy 2024–2029 and the Cybersecurity Strategy 2025–2028, which identify energy, transport, healthcare, water, ICT, financial services, food supply, and public administration as important components of national resilience and essential services. The National Security

Strategy also explicitly emphasizes the need to consider *interdependencies, cascading effects, and secondary impacts* in strengthening the resilience of energy supplies (Government of the Republic of North Macedonia, 2024; Ministry of Digital Transformation, 2024).

The interdependency framework presented in Figure 3 illustrates that energy infrastructure can be considered a foundational node within a wider network of critical infrastructure sectors. Electricity and energy supply support the operation of information and communication technology, transportation systems, healthcare facilities, water services, financial services, food supply chains, and public administration. The importance of energy continuity is further demonstrated by national energy indicators. According to the State Statistical Office**,** 63.2% of gross inland energy consumption in 2023 was supplied by imports, while energy import dependence increased to 65.5% in 2024 (State Statistical Office of the Republic of North Macedonia, 2025a, 2025b). The country's experience during the 2021–2023 energy crisis also demonstrated the cross-sector importance of energy supply, with government measures supporting electricity availability for essential services, including healthcare, water utilities, and other public services (Ministry of Finance of the Republic of North Macedonia, 2022).

Based on these national sources and the interdependency framework presented in Figure 3, the strength of these dependencies can be represented using a three-level scale: *1 = low dependency, 2 = moderate dependency, and 3 = high dependency.* The resulting assessment provides a simplified representation of potential cascading pathways and allows sectors with greater systemic significance to be distinguished from those in which existing buffers or alternative operational arrangements may delay the effects of an energy disruption.

Table 2 summarizes the indicative energy dependency, potential propagation speed, and cascading significance of selected critical infrastructure sectors in North Macedonia, providing a simplified representation of the cross-sector relationships discussed above. It should be stressed that local backup autonomy, dependency strengths, and restoration times have not been verified. The classifications therefore support identifying dependencies for investigation rather than a validated ranking of investment priorities.

Table 2. Indicative energy dependency and cascading significance of selected critical infrastructure sectors in North Macedonia

Critical infrastructure sector	Dependency on energy	Potential propagation speed	Potential cascading significance
Information and communication technology (ICT)	3 – High	Very fast	Very high
Transportation	3 – High	Moderate	Very high
Healthcare	3 – High	Moderate	High
Water	3 – High	Moderate	High
Financial services	3 – High	Fast	High
Food supply	2 – Moderate	Slow	High
Public administration	2 – Moderate	Moderate	High

(Source: Authors' qualitative synthesis of State Statistical Office of the Republic of North Macedonia, 2025a, 2025b; ENTSO-E, 2026)

The assessment presented in Table 2 indicates that ICT and transportation have very high potential cascading significance in the event of an energy disruption. ICT is characterized by very fast propagation, while transportation may experience more moderate propagation due to the availability of certain backup and buffering capacities. Water, healthcare and financial services combine high energy dependency with moderate and fast propagation, respectively, while food supply and public administration may experience slow and moderate service degradation. Overall, the assessment highlights the central role of energy infrastructure and the

different ways in which disruptions may propagate across interconnected critical sectors in North Macedonia.

The simplified assessment demonstrates the value of incorporating interdependency mapping into national critical infrastructure risk assessment. Rather than considering each infrastructure sector independently, decision-makers can identify those cross-sector relationships through which a disruption may produce disproportionate systemic consequences. For North Macedonia, this provides a basis for prioritizing redundancy, backup capacity, alternative communication channels, cross-sector information sharing, and coordinated contingency planning.

4. Discussion

The increasing complexity of critical infrastructure systems necessitates a shift from sector-specific protection measures toward integrated resilience strategies (Weber et al., 2023; Ministry of Digital Transformation, 2024). Traditional approaches focused primarily on preventing individual failures. While prevention remains important, contemporary resilience frameworks must also emphasize adaptation, response, and recovery capabilities.

The European regulatory framework increasingly reflects the need to address critical infrastructure risks through both cybersecurity and broader resilience measures. Directive (EU) 2022/2555 (NIS2) establishes cybersecurity risk-management and reporting requirements for entities operating in critical sectors, while Directive (EU) 2022/2557 on the resilience of critical entities (CER) adopts a broader resilience perspective encompassing prevention, protection, response, mitigation, absorption, adaptation, and recovery (European Parliament and Council of the European Union, 2022a, 2022b). Importantly, the CER Directive explicitly recognizes cross-sectoral interdependencies and hybrid threats as relevant components of critical entity risk assessment. These developments reinforce the need for integrated approaches that combine cyber-physical security, interdependency analysis, and resilience planning.

For North Macedonia, strengthening resilience requires a comprehensive understanding of national infrastructure interdependencies and potential cascading failure pathways. The dependency mapping presented in Section 3.1 illustrates the importance of considering energy infrastructure not as an isolated sector, but as a central component of a broader system of interconnected critical infrastructure. Given this central role, particular attention should be devoted to protecting key energy assets and ensuring continuity of operations during crises (ENER, 2022; Government of North Macedonia, 2024).

Cross-sector cooperation represents one of the most important enablers of critical infrastructure resilience (Government of North Macedonia, 2024). Infrastructure operators, government institutions, emergency services, cybersecurity organizations, and regulatory bodies must develop mechanisms for information sharing, coordinated planning, and joint response activities. Such collaboration enhances situational awareness and improves the ability to manage complex incidents involving multiple sectors.

Redundancy and diversification also play a critical role in resilience enhancement. Distributed energy generation, alternative communication channels, backup operational capabilities, and diversified supply chains can reduce dependence on single points of failure and limit the propagation of disruptions.

Furthermore, resilience planning should recognize the growing importance of the information environment. Hybrid threats frequently exploit public perceptions, misinformation, and institutional trust. Effective communication strategies therefore constitute an essential component of critical infrastructure protection and crisis management. Ultimately, national

resilience depends not only on the strength of individual infrastructure sectors but also on the ability of the broader system to absorb disturbances, adapt to changing conditions, and recover from disruption.

Finally, an important element of resilience is the continuous mapping and monitoring of critical infrastructure interdependencies. Because dependencies evolve alongside digital transformation, periodic reassessment of critical nodes and cross-sector relationships enables decision-makers to identify emerging vulnerabilities before they develop into systemic risks. Integrating dependency analysis into national risk assessment frameworks can therefore improve preparedness and support more effective prioritization of protective investments. Scenario-based planning and stress-testing exercises provide valuable opportunities to identify vulnerabilities before they are exploited. By examining plausible disruption scenarios and their cascading consequences, stakeholders can develop more robust preparedness and response strategies.

Figure 4 summarizes the main resilience-enhancement measures discussed in this section, emphasizing an integrated approach to the protection of energy-centric critical infrastructure. These measures include strengthening redundancy and diversification, continuously monitoring infrastructure interdependencies, improving cross-sector coordination and information sharing, and enhancing preparedness through scenario-based planning. Taken together, these measures support the ability of critical infrastructure systems to anticipate, withstand, respond to, and recover from hybrid threats and cascading disruptions.



Figure 4. Resilience enhancement framework

4.1 Operationalizing Resilience in North Macedonia

A phased programme is needed to translate this framework into accountable action. The Government should designate a cross-sector coordination mechanism linking the Crisis Management Centre, Ministry of Energy, Ministry of Digital Transformation, relevant sector ministries and regulators, and operators. The operator of the electricity transmission system in North Macedonia (MEPSO) - should lead transmission-system dependency and restoration planning, with distribution and generation operators contributing local supply and recovery information. Transportation hubs, hospitals, water utilities, telecommunications providers, financial-service operators, and municipalities should identify essential functions and nominate continuity officers. Cyber-incident coordination should use the competent authorities and CSIRT arrangements under national law, including MKD-CIRT within its remit.

During the first six months after programme approval, the coordination mechanism should agree a protected dependency register, escalation contacts, essential-service priorities, and minimum reporting fields. Operators should record their upstream electricity and communication dependencies, tested backup endurance, fuel-resupply arrangements, and maximum tolerable service interruption. A proposed initial target is a completed and operator-signed dependency record for every participating essential-service operator, with quarterly review of missing records. Sensitive asset details should remain access-controlled; aggregate findings can support national risk assessment.

Between months 6 and 12, operators should test generator transfer, fuel access, alternative communications, and recovery of critical control systems under loss of electricity and telecommunications. MEPSO should coordinate contingency and restoration exercises with neighbouring system operators across existing interconnections and account separately for the North Macedonia–Albania project, reported as entering construction in 2026 (MEPSO, 2026). Cross-border capacity can provide support but also transmit disturbances; it should not be assumed available during a region-wide event. Exercises should include unavailable imports, voltage-control constraints, and competing restoration priorities, drawing on the regional and national investigations (ENTSO-E, 2025, 2026).

Between months 12 and 24, the Government and regulators should review exercise findings and prioritize funded continuity upgrades. A yearly joint exercise should assess time to detect and escalate disruption, time to establish a shared situation report, percentage of critical sites meeting their agreed backup-endurance target under load, essential-service restoration time, and closure of corrective actions. Initial baselines should be established during the first exercise; targets should then be agreed by sector and audited annually. A proposed accountability target is assignment of an owner and deadline to every exercise finding within 30 days, with quarterly reporting of overdue actions. These metrics measure demonstrated service continuity rather than the number of plans produced.

Moreover, alignment with NIS2 and CER should be explicit but legally differentiated. North Macedonia is not an EU Member State, and so EU transposition deadlines do not automatically constitute domestic obligations. Its 2025 Law on Security of Networks and Information Systems and the Ministry's 2026 account of NIS2-aligned reform provide the national cybersecurity context (MKD-CIRT, 2025; Ministry of Digital Transformation, 2026). Implementation must follow the applicable domestic law and designated authorities. CER is used here as an alignment benchmark; the ENER (2022) draft should not be treated as evidence that a CER-equivalent regime is fully implemented.

For NIS2 alignment, participating operators should connect management oversight and training (Article 20) to risk analysis, incident handling, continuity, supply-chain security, and assessment of control effectiveness (Article 21). Exercises should test Article 23 reporting benchmarks for significant incidents: an early warning within 24 hours, notification within 72 hours of awareness, and a final report within one month after notification, subject to the directive's applicable exceptions. For CER alignment, the dependency register should support national cross-sector and cross-border risk assessment (Article 5), identification of critical entities (Article 6), entity risk assessment (Article 12), proportionate resilience measures (Article 13), and disruption notification (Article 15). Cyber and physical resilience leads should exchange assessments and incident information so that overlapping risks are handled coherently (European Parliament and Council of the European Union, 2022a, 2022b).

4.2 Limitations and Future Quantitative Assessment

This review is conceptual, energy-centric, and limited to selected sectors. Electricity interruptions dominate the screening scenario, while gas and fuel pathways receive illustrative treatment. Sector aggregation obscures geographic variation, unequal backup provision, vulnerable populations, and service-specific exceptions. Public incident reports help establish plausible mechanisms but do not demonstrate the frequency of cascades, establish hostile attribution for natural or technical events, or validate the national classifications. Tables 1–2 should consequently guide data collection and scenario design rather than predict losses or justify a precise priority ranking.

Future work should construct a directed, time-dependent multilayer model of electricity, communications, water, healthcare, and selected supply chains, using operator-verified dependencies, electricity-flow constraints, backup duration, fuel logistics, and repair resources. Stress tests should compare localized electricity loss, concurrent communication failure, unavailable cross-border support, and prolonged regional disruption. Sensitivity analysis should vary outage duration, backup failure, dependency thresholds, and restoration order; uncertainty should be reported rather than hidden in a single score. Model outputs could include essential-service downtime, population-hours without service, unmet critical load, and recovery trajectories. Calibration against recorded incidents and independent operator review would be needed before using results for investment decisions.

5. Conclusion

The increasing interconnectedness of modern critical infrastructure systems has created new vulnerabilities that can be exploited through hybrid threats. Because the energy sector serves as a foundational enabler for numerous critical services, disruptions affecting energy infrastructure have the potential to generate cascading failures across multiple sectors. The analysis presented in this paper highlights the importance of understanding infrastructure interdependencies and their implications for national resilience. Hybrid threats targeting energy infrastructure should not be viewed solely as sector-specific challenges. Rather, they represent systemic risks capable of affecting transportation, communications, healthcare, water supply, finance, public administration, and broader societal stability.

The findings provide answers to the three research questions. Hybrid threats targeting energy infrastructure can generate cascading failures through interconnected critical sectors. In North Macedonia, ICT, healthcare, and water sectors, based on the reviewed sources, are provisionally classified as having particularly high potential cascading significance, with ICT also characterized by very fast propagation, while transportation and financial services are assigned moderate and fast propagation, respectively.

Addressing the challenge of cascading failures across the critical infrastructure sectors requires integrated approaches that combine infrastructure protection, cybersecurity, resilience planning, emergency preparedness, and strategic communication. The proposed national programme connects dependency mapping to assigned responsibilities, cross-border coordination, tested continuity, and NIS2/CER alignment. However, until empirical validation is available, the tables and this paper as a whole remain qualitative screening tools. Future research should as a consequence, quantitatively stress-test the identified dependencies using operator or expert verified network and continuity data, explicit propagation delays, and uncertainty analysis that will form central elements of national critical infrastructure protection strategies. In the meantime, strengthening resilience in energy-centric critical infrastructure remains essential for national security, economic stability, and societal well-being.

Acknowledgment

This paper's publishing and presentation were funded by Military academy "General Mihailo Apostolski" – Skopje.

References

Buldyrev, S. V., Parshani, R., Paul, G., Stanley H. E. & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature 464*, 1025–1028, https://doi.org/10.1038/nature08932

Cimellaro, G. P., Cardoni, A., & Reinhorn, A. (2024). Modelling infrastructure interdependencies and cascading effects using temporal networks. *Resilient Cities and Structures*, 3 (3), 28–42, https://doi.org/10.1016/j.rcns.2024.05.002

CISA, FBI, and NSA. (2022). *Understanding and mitigating Russian state-sponsored cyber threats to U.S. critical infrastructure* (Joint Cybersecurity Advisory AA22-011A). Available: https://www.cisa.gov/news-events/alerts/2022/01/11/understanding-and-mitigating-russian-state-sponsored-cyber-threats-us-critical-infrastructure

Council of the European Union. (2022). *Declaration by the High Representative on behalf of the European Union on leaks in the Nord Stream gas pipelines*. Available: https://www.consilium.europa.eu/en/press/press-releases/2022/09/28/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-leaks-in-the-nord-stream-gas-pipelines/

Danish Energy Agency. (2022). *Nord Stream 1 genåbner ikke som planlagt: Forsyningssikkerheden er fortsat under pres* [Nord Stream 1 does not reopen as planned: Security of supply remains under pressure]. Available: https://ens.dk/presse/nord-stream-1-genaabner-ikke-som-planlagt-forsyningssikkerheden-er-fortsat-under-pres

ENTSO-E. (2025). *ENTSO-E publishes the final report on the grid incident in South-East Europe*. Available: https://www.entsoe.eu/news/2025/02/25/entso-e-publishes-the-final-report-on-the-grid-incident-in-south-east-europe/

ENTSO-E. (2026). *ENTSO-E publishes Expert Panel final report on 18 May 2025 blackout in North Macedonia*. Available: https://www.entsoe.eu/news/2026/04/20/entso-e-publishes-expert-panel-final-report-on-18-may-2025-blackout-in-north-macedonia/

European Parliament and Council of the European Union. (2022a). Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

European Parliament and Council of the European Union. (2022b). Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities (CER Directive). *Official Journal of the European Union.* Available: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

Federal Energy Regulatory Commission (FERC). (2021). *Final report on February 2021 freeze underscores winterization recommendations*. Available: https://www.ferc.gov/news-events/news/final-report-february-2021-freeze-underscores-winterization-recommendations

Gjorgjievska, T. (2025). Assessing the vulnerabilities of critical infrastructure in the age of hybrid threats. *Security Dialogues.* 16 (2), 33, https://doi.org/10.47054/SD25233gj

Gong, S., Ye, Y., Gao, X., Chen, L., & Wang, T. (2023). Empirical patterns of interdependencies among critical infrastructures in cascading disasters: Evidence from a comprehensive multi-case analysis. *International Journal of Disaster Risk Reduction*, 95, 103862, https://doi.org/10.1016/j.ijdrr.2023.103862

Government of the Republic of North Macedonia (2024). National security strategy of the Republic of North Macedonia (2024–2029). Skopje, 2024. Available: https://portal.mdt.gov.mk/post-body-files/nacionalni-strategii-file-vxaq.pdf

Heracleous, C., Kolios, P., Panayiotou, C. G., Ellinas, G., & Polycarpou, M. M. (2017). Hybrid systems modeling for critical infrastructures interdependency analysis, *Reliability Engineering & System Safety,* 165, 89-101, https://doi.org/10.1016/j.ress.2017.03.028

Huang, Z. (2014). Interdependent cyber-physical systems: Robustness and cascading failures (*Doctoral dissertation*). Ottawa-Carleton Institute for Electrical and Computer Engineering, School of Electrical Engineering and Computer Science, Faculty of Engineering, University of Ottawa, Canada.

Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A., & Giannopoulos, G. (2023). Hybrid threats: A comprehensive resilience ecosystem, *Publications office of the European Union*, https://data.europa.eu/doi/10.2760/37899

Kaspersky ICS CERT. (2025). A brief overview of the main incidents in industrial cybersecurity Q4 2024. Available: https://ics-cert.kaspersky.com/publications/reports/2025/04/08/q4-2024-a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity/

MEPSO. (2026). *Construction begins on the 400 kV North Macedonia–Albania interconnection line*. Available: https://www.mepso.com.mk/index.php/en/component/content/article/114-en-category/doma/vesti-i-aktuelnosti/937-construction-begins-on-the-400-kv-north-macedonia-albania-interconnection-line

Ministry of Digital Transformation (2024). Cybersecurity strategy of the Republic of North Macedonia 2025-2028. Skopje, 2024. Available: https://mdt.gov.mk/mk-MK/regulativa/strategija-za-sajber-bezbednost

Ministry of Digital Transformation. (2026). *Andonovski: The new law on cybersecurity establishes a system of resilience also in the private sector – the obligations are shared*. Available: https://mdt.gov.mk/en-GB/odnosi-so-javnost/soopstenija/andonovski-noviot-zakon-za-sajber-bezbednost-vospostavuva-sistem-na-otpornost-i-vo-privatniot-sektor-obvrskite

Ministry of Finance of the Republic of North Macedonia. (2022). Energy crisis, price increase and government policies: Timing, scope and targeting. Skopje.

MKD-CIRT. (2025). *Law on Security of Networks and Information Systems – 2025* [in Macedonian]. Available: https://mkd-cirt.mk/download/zakon-za-bezbednost-na-mrezi-i-informaciski-sistemi-2025/

National legislature registry (ENER) of North Macedonia (2022). Draft law on critical infrastructure. Available: https://ener.gov.mk/Default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=77229

Noebels, M. (2022). Assessment and enhancement of power grid resilience to shocks and stresses (*Doctoral Dissertation*), University of Manchester. Available:

https://research.manchester.ac.uk/en/studentTheses/assessment-and-enhancement-of-power-grid-resilience-to-shocks-and/

Olorunlana, T. J., & Mohammed, H. (2025). Analysis of the Colonial Pipeline cybersecurity incident. *International Journal of Science, Architecture, Technology, and Environment*, 2 (4), https://doi.org/10.63680/jngh0767as

Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, vol. 121, pp. 43–60, https://doi.org/10.1016/j.ress.2013.06.040

Pant, R., Thacker, S., & Hall, J.W. (2017). System-of-systems framework for global infrastructure vulnerability assessments. *Fifth Green Growth Knowledge Platform Annual Conference*, November 27-28, Washington DC, US. Available: https://www.greenpolicyplatform.org/research/system-systems-framework-global-infrastructure-vulnerability-assessments

Rinaldi, S. M., Peerenboom, J. P. & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21 (6), 11-25, https://doi.org/10.1109/37.969131

Srinivasan, S., & Ni, L. K. (2023). Ransomware attack at Colonial Pipeline Company (Harvard Business School Case No. 123-069). *Harvard Business School Publishing*. Available: https://www.hbs.edu/faculty/Pages/item.aspx?num=63756

State Statistical Office of the Republic of North Macedonia. (2025a). Energy balances, 2023 – definitive data. Skopje. Available: https://www.stat.mk/en/stat/industry-energy-and-environment/energy/energy-balances/energy-balances-2023-definitive-data

State Statistical Office of the Republic of North Macedonia. (2025b). Energy balances, 2024 – preliminary data. Skopje. Available: https://www.stat.mk/en/stat/industry-energy-and-environment/energy/energy-balances/energy-balances-2024-preliminary-data

U.S. Department of Energy and U.S. Department of Homeland Security. (2018). *Executive Order 13800 on strengthening the cybersecurity of federal networks and critical infrastructure: Assessment of electricity disruption incident response capabilities*. Available: https://www.energy.gov/articles/executive-order-13800-strengthening-cybersecurity-federal-networks-and-critical

Wang, Y., Zhao, O., & Zhang, L. (2024). Multiplex networks in resilience modeling of critical infrastructure systems: A systematic review. *Reliability Engineering & System Safety*, 250, 110300, https://doi.org/10.1016/j.ress.2024.110300

Weber, V., Pericàs Riera, M., & Laumann, E. (2023). Mapping the world's critical infrastructure sectors. *DGAP Policy Brief No. 35.* German Council on Foreign Relations. Available: https://dgap.org/en/research/publications/mapping-worlds-critical-infrastructure-sectors

Zio, E. & Sansavini, G. (2011). Modeling interdependent network systems for identifying cascade-safe operating margins, *IEEE Transactions on Reliability*, vol. 60, no. 1, pp. 94-101, March 2011, https://doi.org/10.1109/TR.2010.2104211