

THE IMPACT OF ASYMMETRIC WARFARE ON THE PROTECTION OF NATIONAL CRITICAL ELECTRICITY INFRASTRUCTURE

Tamás SZALÓKI

Ludovika University of Public Service, Budapest, Hungary

szalokitt@gmail.com

ORCID: 0009-0008-3325-1144

ABSTRACT

This study examines the evolution of warfare targeting from the Yugoslav conflicts to the ongoing conflicts in Ukraine and the Middle East within the electricity sector. The author highlights that attacks against electrical power networks are intended to break societal morale and paralyze state administration. The 2026 Middle East escalation is analyzed as a second empirical theater which, together with the Ukrainian record, provides cross-theater validation of the identified targeting patterns and of the underlying economic logic. The paper develops an original parametric cost model to quantify the economic asymmetry generated by low-cost drone technology, introducing three derived indicators: the Cost-Exchange Ratio, the Interception Economy Index, and the Resilience Break-Even Point. The model is extended probabilistically to establish a critical attack intensity threshold above which decentralized resilience investment becomes economically rational. The study further establishes that the emerging layer of directed energy weapons, while correcting the marginal engagement economy, does not correct the defender's aggregate exposure, and that its availability is recursively dependent on the local power autonomy it is deployed to protect. The primary objective of this article is to contribute to the iterative development of national strategic resilience methodologies and defense protocols, while enhancing operational preparedness to mitigate the effects of asymmetric kinetic strikes and systemic cascading failures at critical infrastructure nodes through the integration of hybrid, mobile, and grid-independent power generation capabilities.

KEYWORDS:

asymmetric warfare, critical infrastructure protection, grid resilience, loitering munitions, mobile generators, cascading failure, autonomous management

Submission Received: 23 June 2026; Revised: 27 July 2026; Accepted: 31 July 2026; Published: September 2026

1. Introduction

In the 21st century, the continuous and resilient supply of electrical power constitutes a fundamental prerequisite for the operation of modern societies. Electrical energy has transcended its role as a mere convenience service to become the mission-critical “technological oxygen” of the digital society. In this hyper-connected operational environment, the electrical power system (EPS) is not merely one infrastructure sector among many, but the universal enabling platform upon which all processes of public administration, national economy, and civil-military sustainment are built.

DOI: 10.2478/raft-2026-0029

© 2026 Tamás Szalóki. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

1.1. Digital Dependency of Generations Y and Z: Cognitive and Social Vulnerability

The digital transformation of society has fundamentally altered the metrics of societal resilience. The vulnerability of the EPS now carries direct psychological and asymmetric risks, particularly for the “digital native” cohorts. For Generations Y and Z, the cyberspace domain is no longer an optional tool but the primary environment for social cohesion and existence.

For these demographic cohorts, the denial of electricity effectively results in the collapse of their entire social identity and communication architecture. This total dependency constitutes a critical soft target in asymmetric warfare; an attack against the grid, therefore, yields not only kinetic destruction but immediate societal incapacitation and panic. The 2025 Spanish blackout operational case study clearly demonstrated this: the disruption of digital services triggered a psychological crisis and mass disorientation within hours, which paralyzed voluntary emergency response efforts and degraded the operational effectiveness of official crisis communication (Castro-Delgado et al., 2025).

1.2. The Risk of Cascading Failures

Deep systemic interdependencies exist between electricity supply and other critical infrastructures. A failure within the EPS is not an isolated event but the trigger for a cascading failure (domino effect), in which electricity serves as the decisive primary node. Once the electricity supply is disrupted, cascading effects propagate across four vital systems.

Once the electricity supply is disrupted, cascading effects propagate across the following vital systems:

1. **Communication Cascade:** The depletion of uninterruptible power supplies (UPS) at base stations, resulting in the total collapse of mobile networks and internet connectivity and severely degrading Command and Control (C2) capabilities (Varga, 2011). This cascade is not merely a technical degradation but a documented determinant of sectoral continuity. Christián et al. (2025) establish for the Hungarian health sector that structured, technology-supported crisis communication is essential to maintaining the continuity of healthcare services and to facilitating effective inter-organizational coordination during emergencies. Since that communication capability is itself electrically dependent, the loss of supply produces a compound effect at the hospital: the institution loses simultaneously its operating energy and the coordination mechanism through which its own degraded state would be managed. This finding is carried forward in Subsection 6.4.2, where it determines the load prioritization hierarchy of the proposed islanding sequence.

2. **Sustainment Cascade:** The failure of drinking water pumps and wastewater treatment systems, which leads to a critical public health crisis within hours.

3. **Logistics Cascade:** Fuel distribution at strategic filling stations ceases, supply chains collapse, and the food supply chain fails due to cold chain disruption.

4. **Financial Cascade:** The financial cascade results from the halt of electronic payment systems, producing immediate economic paralysis and civil unrest, potentially escalating into looting and internal security threats.

This cascading effect directly threatens the Operational Continuity of Government (COG). This study demonstrates that in the era of asymmetric warfare, strikes against electrical networks have become primary strategic tools because they enable the adversary to generate maximum societal and governmental chaos with minimal kinetic expenditure.

1.3. Asymmetric Threat and Strategic Resilience

The Ukraine conflict (2022-2026) and the recent Middle Eastern escalations demonstrated that centralized high-voltage transmission networks are inherently vulnerable to modern asymmetric threats. The adversary deliberately targets the “trigger points” of cascading failure: high-value substations whose destruction initiates system-wide functional degradation. The objective of this study is to demonstrate that traditional, static, and centralized defense doctrines are no longer capable of mitigating such cascading effects. Strategic resilience is not defined by the invulnerability of the network, but by the ability to sustain operations through decentralized, technologically hybrid capabilities. Advanced systems, such as grid-synchronized mobile generators and high-capacity Electrochemical Battery Energy Storage Systems (BESS), are required to intercept and contain cascading failures at critical nodes. At the 2026 threat level, national sovereignty and mission readiness depend on the capability of critical institutions to transition into autonomous, synchronized island-mode operation within seconds of a UAS (Unmanned Aerial System) strike, thereby severing the path of cascading failures (IEA, 2024).

2. Materials and Methods

To fulfill the research objectives and formulate a scientifically substantiated proposal for national energy security, a multi-layered methodology was employed, integrating historical analysis, operational modeling, and technological synthesis. The research is structured upon five methodological pillars:

- Comparative Historical and Doctrinal Analysis: The research commenced with a comprehensive review of the evolution of energy warfare. By contrasting the “soft kill” graphite-based operations of the 1990s with the “hard kill” kinetic attrition observed in the 2022-2026 Ukrainian theater, the study identifies recurring adversary targeting patterns directed at high-voltage transmission nodes.
- Operational Case Study Analysis: The 2025 Spanish blackout served as the primary operational case study to model cascading failure propagation in contemporary low-inertia grids. This method enabled the identification of critical time windows where autonomous intervention, utilizing Battery Energy Storage Systems and synchronous generators is required to avert total systemic collapse. The 2026 Middle East escalation is analyzed as a second operational case study: the documented system-level damage data of the Iranian grid and the reciprocal targeting of the Israeli system are used to validate, in a second theater, the attrition patterns and the criticality-based target selection logic identified in Ukraine (Subsection 3.4).
- Legal and Regulatory Review. The study examines the current European regulatory framework, with specific emphasis on the EU CER (Critical Entities Resilience) Directive, to ensure that the proposed technological solutions align with national sovereignty and Continuity of Government (COG) requirements.
- Quantitative Cost-Exchange Modeling: An original parametric cost model was constructed to quantify the economic asymmetry of UAS-based attrition against national transformer stations. Rather than reproducing previously published unit costs, the model introduces three derived indicators, namely the Cost-Exchange Ratio, the Interception Economy Index, and the Resilience Break-Even Point, computed from open-source unit-cost ranges and from the macroeconomic outage-loss coefficients published by Wing et al. (2025). The model is subsequently extended probabilistically to derive a critical attack intensity threshold. It is parametric rather than deterministic: all input ranges are stated explicitly, and the resulting ratios are presented as order-of-magnitude findings robust to variation within the published cost bands. The purpose of

the model is not to predict absolute damage values, but to establish the direction and scale of the economic imbalance, and to identify the threshold at which decentralized resilience investment becomes economically rational.

- **Synthesis of Civil-Military Synergies:** This method was utilized to merge civil-sector technological capabilities (including market-based BESS and synchronous generators) with military logistical frameworks. This integration was modeled to evaluate the cost-effectiveness and operational feasibility of the proposed strategic investment (UNECE, 2015).

By employing these methodologies, the study provides a comprehensive framework that bridges the gap between theoretical defense doctrines and practical engineering applications for 21st-century energy security.

3. Historical Overview

Targeted physical attacks against the Electrical Power System (EPS) are not a nascent phenomenon but rather a mature doctrinal operational practice spanning over three decades. Contemporary combat operations confirm that neutralizing an adversary's power infrastructure with relatively low resource expenditure yields disproportionately high strategic impact: it degrades Command and Control (C2) nodes, compromises Integrated Air Defense Systems (IADS), erodes the resilience of the strategic hinterland, and compels political concessions. This chapter analyzes historical precedents to identify patterns of low-cost physical attacks and derives strategic conclusions for national defense.

3.1. The Gulf War (1991). The Doctrinal Baseline

The first large-scale application of modern, targeted electrical warfare occurred during Operation Desert Storm. On the initial day of the air campaign, coalition forces deployed Tomahawk Land Attack Missiles (TLAM) equipped with Kit-2 payloads containing carbon-graphite filaments. These were dispersed over Iraqi switching and transformer stations, inducing immediate system-wide short circuits. The operational results highlighted the systemic vulnerability of the EPS:

- Approximately 85 per cent of Iraq's generating capacity was immediately taken offline;
- Out of 20 major power plants, 11 were destroyed and 6 were severely damaged; and total production plummeted to 4 per cent of pre-war levels by the end of the campaign;
- At the Baiji plant, only two Tomahawk strikes successfully neutralized nearly 10 per cent of the national supply (Glosson, 1993).

The subsequent cascading failure collapsed water treatment and sewage systems, triggering a protracted humanitarian crisis.

The doctrinal takeaway established that neutralizing dual-use power infrastructure acts as a force multiplier – it is more cost-effective than direct attrition of maneuver units and accelerates political collapse by targeting civilian sustainment.

3.2. The Yugoslav War. The “Soft Kill” Paradigm

During the Kosovo crisis, NATO evolved the 1991 model: the objective shifted from permanent destruction to temporary but total incapacitation. In May 1999, F-117 Nighthawks deployed CBU-94 “Blackout Bombs” (containing BLU-114/B graphite submunitions) against five Yugoslav power plants.

Over 70 per cent of the national grid was neutralized within minutes, plunging Belgrade, Novi Sad, and Nis into darkness (Anđelković-Lukić et al., 2024).

This engagement provided two critical lessons for defense planning. First, the grid can be neutralized using non-lethal, low-cost assets. Second, overhead transmission lines remain structurally defenseless against dispersed graphite agents, as wide-scale insulation of high-voltage lines is economically and technically unfeasible.

3.3. The Russia-Ukraine War (2022-2026). Mass-Scale Asymmetric Attrition

The Ukrainian theater represents the first European instance of sustained, systemic attrition against an EPS. The adversary systematically targeted 750 kV and 330 kV substations, effectively severing the hinterland from its generation base (Kovács, 2024).

The common denominator between the 2026 Middle Eastern escalation and the Ukrainian experience is the proliferation of One-Way Attack (OWA) Unmanned Aerial Systems (UAS), such as the Shahed-136. These assets, costing between 20,000 and 50,000 USD, are capable of destroying multi-million dollar transformer stations, creating a severe economic asymmetry of destruction. Ukraine mitigated this functional degradation by deploying over 130,000 decentralized, off-grid (island-mode) generator sets, proving the strategic necessity of distributed energy reserves (IEA, 2024).

3.4. The 2026 Middle East Escalation: Cross-Theater Validation of the Attrition Pattern

The escalation that commenced in February 2026 between the United States and Israel on one side and Iran on the other constitutes the second contemporary theater, after Ukraine, in which energy infrastructure was elevated to a primary strategic target set. Its doctrinal precursor, the twelve-day war of June 2025, already exhibited the signature of precision attrition defined in Subsection 4.2: individual low-cost unmanned aerial vehicles struck the onshore Phase 14 processing section of the South Pars gas field and the Fajr-e Jam gas processing plant, demonstrating that single sub-50,000 USD assets could interrupt production at nodes of national significance. The 2026 campaign industrialized this pattern. Within the first four weeks of hostilities, at least forty oil and gas facilities across the region had been severely damaged according to the assessment of the International Energy Agency, and by the conclusion of the approximately forty-day campaign the target set had expanded from fuel-chain assets to generation plants, transmission infrastructure and large industrial consumers (Human Rights Watch, 2026; PBS News, 2026).

From a power engineering perspective, the Iranian case introduces a targeting dimension absent from the Ukrainian record: the exploitation of gas-electric coupling. Approximately eighty per cent of Iranian generation is fueled by natural gas, and the share of thermal generation exceeds ninety per cent (PBS News, 2026). The Israeli strike of 18 March 2026 against the South Pars field was therefore not an attack on the hydrocarbon export economy alone but an indirect attack on generation adequacy: by degrading the primary energy conversion chain upstream of the busbar, the attacker removes dispatchable megawatts without expending a single munition against a transformer station. This extends the cascade logic developed in Subsection 1.2 in the upstream direction, and it implies that the vertex set of the criticality model formulated in Subsection 5.1.4 must, for gas-dominated systems, be augmented with fuel-supply nodes whose removal propagates into the electrical domain with a delay determined by linepack and storage inventories rather than by protection-system timescales.

The aggregate damage figures reported for the Iranian grid provide the first quantified, system-level dataset of a contemporary strategic energy campaign outside Ukraine. The state transmission and distribution company Tavanir reported a 4,200-megawatt reduction in available generating capacity, damage at more than two thousand distinct points of the national network, and direct sectoral losses of approximately one billion USD (Al Jazeera, 2026). The research service of the Iranian parliament projected a peak summer deficit of 13,640 megawatts against a maximum simultaneous supply of approximately 68,420 megawatts and a peak demand exceeding 81,000 megawatts, with industrial zones subjected to rationing of four to six hours per day (Iran International, 2026; Al Jazeera, 2026). Two analytical findings follow. First, damage distributed across more than two thousand network points defeats centralized repair logistics for precisely the reason identified in Subsection 5.1.2: replacement of high-voltage equipment is constrained by manufacturing lead times measured in months, and no national spares inventory is dimensioned for a four-digit damage-point count. Second, the campaign reshaped both sides of the supply-demand balance simultaneously. The forced outage of the Mobarakeh and Khouzestan steel works notionally returned some two thousand megawatts of load to the balance, yet the strike on the Mahshahr petrochemical complex converted a node that had previously exported surplus generation into a net consumer (Al Jazeera, 2026). In a deeply coupled industrial grid, kinetic attrition thus modifies the load-flow problem on both the generation and the demand side, a phenomenon not observed in Ukraine, where damage was concentrated at the transmission level.

The reciprocal targeting of the Israeli system validated the criticality-maximization logic formalized in Subsection 5.1.4 under conditions of a highly capable, layered air defense. Iranian ballistic missile attacks were directed against the Orot Rabin complex near Hadera, the largest generation site of the country, without achieving a hit; the Bazan refinery in Haifa was struck with brief disruption to local supply; and a high-voltage line at Rosh Ha'ayin was damaged, causing a localized outage (The Times of Israel, 2026). Of greater doctrinal significance is the reported transfer of targeting intelligence: according to information attributed to Ukrainian intelligence sources, Russia provided Iran with a structured list of fifty-five Israeli energy targets organized in a three-tier hierarchy descending from national generation assets through transmission infrastructure to regional substations, together with the assessment that the isolated, non-interconnected character of the Israeli system implies that the loss of a small number of central components could precipitate a prolonged national collapse (The Jerusalem Post, 2026). Two conclusions follow for European defense planning. First, targeting doctrine matured in the Ukrainian theater is being transferred between belligerents as a codified product, and the raid-intensity parameter of Subsection 5.1.4 therefore cannot be treated as theater-specific. Second, synchronous interconnection is itself a resilience asset, since an interconnected system can import both energy and inertia across the disturbance; yet interconnection lies outside the control of the defending state and can be curtailed by the failure or policy of neighbors, which reinforces rather than weakens the argument for autonomous node-level capability developed in Section 6.

Finally, the escalation internationalized the cascade. Iranian retaliation extended to third states: the Ras Laffan liquefied natural gas facility in Qatar, which supplies approximately one fifth of the global LNG market, was struck on two consecutive days, a drone strike ignited a fuel depot at Kuwait International Airport, and interceptions of transiting missiles and unmanned aerial vehicles were confirmed over Saudi Arabia,

the United Arab Emirates and Bahrain (Human Rights Watch, 2026; The Times of Israel, 2026). The propagation graph of Subsection 5.1.4 must therefore, in principle, be extended beyond national boundaries: fuel-chain nodes of global significance couple national electricity systems through markets and fuel logistics even where no synchronous electrical connection exists. For the model developed in Section 5, the 2026 theater supplies qualitative validation on four points: the effectiveness of mixed strike profiles combining ballistic missiles, cruise missiles and One-Way Attack unmanned systems against saturated defenses; the viability of fuel-chain targeting as an indirect attack on generation adequacy; the simultaneous reshaping of supply and demand in industrialized grids; and the diffusion of targeting doctrine through intelligence transfer. Jointly these confirm that the critical attack intensity threshold derived in Subsection 5.1.4 is a conservative bound for any centralized, weakly redundant national system.

3.5. International Legal Framework and the Protection of Civilian Infrastructure

The legality of strikes against the EPS is governed by International Humanitarian Law (IHL), yet it remains a highly contested domain. The primary reference is the 1977 Additional Protocol I to the 1949 Geneva Conventions.

- The Principle of Distinction: Belligerents must distinguish between the civilian population and combatants, and between civilian objects and military objectives. Under Article 52(2), attacks must be limited to military objectives. While the EPS often supports military facilities, its primary function remains civilian.

- The Dual-Use Dilemma: Aggressors frequently argue that the EPS constitutes a legitimate military objective due to its role in powering C2 and AD systems. However, IHL dictates that an attack is only lawful if the concrete and direct military advantage outweighs the incidental injury to civilians. Neutralizing health care and basic survival systems by denying electricity is often viewed as a violation of the principle of proportionality.

- Objects Indispensable to Survival: Article 54 prohibits the destruction of objects indispensable to the survival of the civilian population. In modern urban environments, water and sanitation cease without electricity. Consequently, systemic strikes against the EPS constitute a direct assault on civilian life.

However, since several key global powers have not ratified this Protocol, these protections often rely solely on Customary International Humanitarian Law. The documented consequences of UAS-based strikes including hospital fatalities and critical water shortages, confirm that despite legal prohibitions, civilian infrastructure remains a primary target in asymmetric warfare (UNECE, 2015).

The conclusion of this legal analysis is determinative for the argument developed in the remainder of the study, and is therefore stated explicitly. The existing international legal framework establishes prohibitions but does not establish protection: it imposes obligations upon belligerents without conferring any enforceable defensive capability upon the targeted state. Where the prohibition is not observed, as the documented evidence indicates it frequently is not, the targeted state possesses no legal remedy that operates within the timescale of the attack. It follows that legal protection cannot constitute the primary layer of critical electricity infrastructure defense, and that the deficit must be compensated by autonomous technological resilience under the exclusive control of the defending state. This conclusion is revisited in Section 7, where it forms one of the premises of the proposed doctrinal shift.

4. Proliferation of Combat-Cost Optimized Unmanned Aerial Systems (UAS)

Traditional doctrines for Critical Infrastructure Protection (CIP) were built for decades upon the principles of geographic separation and Layered Air Defense. It was assumed that national strategic assets located in the strategic depth's – such as high-voltage substations – remained secure far from the forward line of own troops (FLOT) or under the protection of expensive anti-ballistic missile shields. However, the mass proliferation of Unmanned Aerial Systems (UAS), specifically One-Way Attack (OWA) drones by the mid-2020s, has fundamentally dismantled these assumptions.

4.1. Erosion of Protected Strategic Depth

The most significant impact of UAS technology is the re-evaluation of operational depth. Modern, long-range loitering munitions have enabled adversaries to strike energy hubs hundreds or even thousands of kilometers behind the front lines. This capability has de facto abolished the “hinterland” as a protected sanctuary in security policy categories.

During the 2026 Middle Eastern escalation, the mass deployment of Shahed-136 type assets demonstrated that any element of the electrical grid is vulnerable across a nation's entire territory. Due to their low-altitude flight profiles, small Radar Cross-Section (RCS), and programmable waypoint navigation, these systems can bypass traditional air defense arrays optimized for high-altitude, high-velocity targets. Consequently, the defense of power infrastructure no longer begins at a geographic border but must be addressed individually at every critical network node (Erazo-Chamorro et al., 2022).

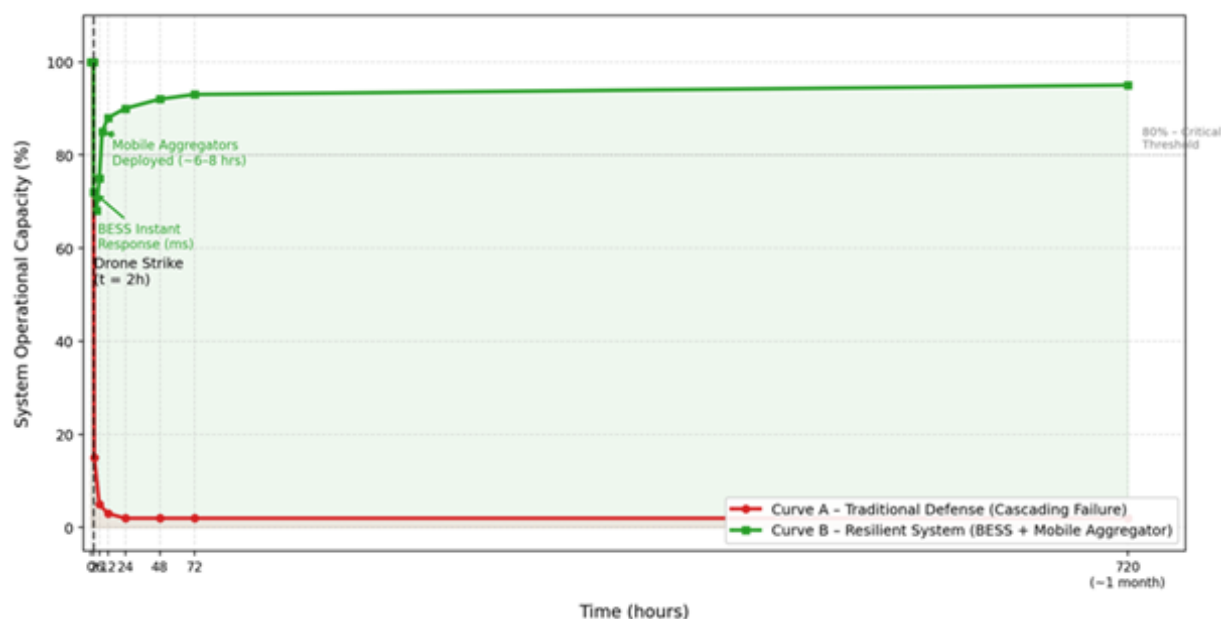


Figure no. 1: Cascading failure vs. Resilient Recovery, Energy Infrastructure Response to Drone Strike
(Source: Author's own illustration based on IEA, 2024)

4.2. Precision Attrition through Target Discrimination

UAS have not only overcome distance but have elevated terminal accuracy to a new dimension. While previous conflicts (e.g., 1991 or 1999) relied on large-area sorties or the dispersal of graphite filaments, modern drone warfare utilizes surgical strikes with centimeter-level precision.

Adversaries now systematically identify the “soft points” of the Electrical Power System (EPS). Neutralizing the cooling system or the control module of a 750 kV autotransformer requires a minimal explosive payload yet results in total functional defeat or long-term incapacitation of the asset.

4.3. Saturation Attack (Swarm) Tactics

The deployment of low-cost drones in swarms is designed to saturate the tracking and engagement capacity of integrated air defense systems. While a high-value surface-to-air missile (SAM) may successfully intercept a target, a coordinated arrival of ten to twenty drones ensures that, statistically, several units will penetrate the defensive screen.

For the EPS, this is a critical vulnerability: a transformer station does not need to be physically leveled; a single successful kinetic impact out of ten is sufficient to plunge a region into darkness. In a European context, the 2025 Spanish Blackout serves as a definitive example. Post-incident analysis revealed that modern SCADA (Supervisory Control and Data Acquisition) and grid management IT architectures are exceptionally sensitive to such disruptions. Beyond physical destruction, the overload of communication channels paralyzed remote restoration efforts, extending the duration of the outage (Garcia-Sanz et al., 2025).

A further consequence follows directly from the saturation logic described above, and it is quantifiable. Because a saturation raid succeeds if a single asset penetrates the defensive screen, the attacker’s effective cost per successful strike does not equal the unit cost of one UAS, but the cost of the entire raid package divided by the number of penetrations achieved. Conversely, the defender’s exposure is not limited to the replacement value of the damaged transformer station, but includes the full macroeconomic cost of the resulting supply interruption. This structural difference between the two cost bases is the mechanism that generates the economic asymmetry, and it can be expressed numerically.

The emergence of UAS has eliminated the immunity of deep-depth territories and transformed the grid into the most vulnerable surface of modern warfare. The combination of precision and mass-scale employability has created a novel threat environment where traditional, static defense is no longer sufficient. This leads to the next critical assessment: the extreme economic asymmetry arising from the use of low-cost combat drones against high-value, finite defensive capabilities and national energy infrastructure.

5. Economic Asymmetry between Low-Cost UAS and Defensive Capabilities

The defining characteristic of asymmetric warfare lies not in technological superiority, but in a profound economic imbalance. Modern strikes against National Critical Electricity Infrastructure function as financial and logistical traps for national defense systems. Relying on traditional kinetic defensive assets leads to long-term, unsustainable economic attrition. This environment is defined by an exponential asymmetry: the counter-positioning of low-cost offensive systems against high-value, finite defensive and recovery capabilities.

5.1. “Pennies for Destruction, Billions for Repair”

Modern energy warfare is predicated on assets such as the Shahed-136 type loitering munitions. The production cost of these units – estimated between 20,000 and

50,000 USD – is negligible compared to the strategic damage they inflict. In contrast, the high-voltage (750/330 kV) transformer stations targeted represent a unit cost of several million dollars, with procurement and manufacturing lead times spanning several months or even a year. Due to the cascading domino effect, the validated cost of a grid failure at the national GDP level can be orders of magnitude higher than the physical damage itself (Zampronha & Albuquerque, 2024).

5.1.1. Definition of the Cost-Exchange Model

To move beyond the qualitative observation that offensive assets are inexpensive, this study defines a parametric cost-exchange model. Three indicators are introduced.

The Cost-Exchange Ratio (CER) expresses the defender's total loss relative to the attacker's expenditure for a single successful engagement:

$$\text{CER} = (C_{\text{hardware}} + C_{\text{cascade}}) / (n \cdot C_{\text{UAS}})$$

where C_{hardware} is the replacement cost of the damaged transformer station including auxiliary switchgear and protection equipment, C_{cascade} is the macroeconomic loss generated by the resulting supply interruption, n is the number of UAS committed to the raid, and C_{UAS} is the unit cost of one One-Way Attack asset.

The Interception Economy Index (IEI) expresses the ratio of the defender's kinetic engagement cost to the attacker's asset cost:

$$\text{IEI} = (k \cdot C_{\text{interceptor}}) / C_{\text{UAS}}$$

where k is the number of interceptors expended per incoming target under the applicable engagement doctrine.

The Resilience Break-Even Point (RBEP), the principal original metric of this study, expresses the number of avoided outage hours at which a decentralized resilience package amortizes against the cascade losses it prevents:

$$\text{RBEP} = C_{\text{resilience}} / L_{\text{hourly}}$$

where $C_{\text{resilience}}$ is the total acquisition cost of the resilience package deployed at the protected node, and L_{hourly} is the hourly macroeconomic loss avoided by maintaining supply at that node.

5.1.2. Reference Scenario and Input Parameters

The model is applied to a reference scenario representative of the Central European operating environment: a saturation raid of ten OWA UAS directed against a single 400/120 kV transformer station supplying a regional load centre of approximately half a million inhabitants. A leaker rate of one penetration in ten is assumed, consistent with the saturation tactics described in Subsection 4.3.

Input values are drawn from published ranges. UAS unit cost is taken at the midpoint of the Zampronha and Albuquerque (2024) band. Transformer replacement cost is taken from the extra-high-voltage range documented by the United States Department of Energy (2012), which places 230 to 765 kV class units at 2 to 10 million USD depending on rating

and specification; the midpoint of this band is applied, increased by 25 per cent to account for station auxiliaries, switchgear and protection systems. Interceptor unit costs are open-source estimates for the surface-to-air missile classes referenced in Subsection 5.2. The hourly cascade loss is derived from the outage-loss coefficients of Wing et al. (2025), scaled to the regional load centre defined above.

Table no. 1
Input parameters of the cost-exchange model

Parameter	Symbol	Value applied	Source basis
UAS unit cost	C_UAS	35,000 USD	Zampronha & Albuquerque (2024), midpoint
UAS committed per raid	n	10	Saturation tactics, Subsection 4.3
Total raid expenditure	$n \cdot C_{\text{UAS}}$	350,000 USD	Computed
Transformer station replacement	C_hardware	approx. 5.6 million USD	DOE (2012) EHV band midpoint plus 25 per cent auxiliaries
Replacement lead time	—	9 to 18 months	DOE (2012)
Interceptor unit cost	C_interceptor	1.0 to 4.0 million USD	Open-source estimates, SAM classes
Interceptors per target	k	1 to 2	Engagement doctrine range
Hourly cascade loss	L_hourly	approx. 1.25 million USD/h	Derived from Wing et al. (2025)
Single-shot probability of kill	p	0.90 to 0.99	Doctrinal range, Subsection 5.1.4
Cascade reduction factor	r	0.90	Modelled, Subsection 5.1.4
Resilience package cost	C_resilience	approx. 12.0 million USD	Computed, Subsection 5.4.1
Service life	T	15 years	Assumed

5.1.3. Computed Results

Applying the reference values, the Cost-Exchange Ratio for a single-day regional interruption is approximately one hundred to one. The hardware loss alone yields a ratio of sixteen to one; the inclusion of cascade losses raises the ratio by an order of magnitude. For a three-day interruption, the duration observed in several documented Ukrainian regional events, the ratio approaches two hundred and seventy to one.

The decisive methodological finding is that the ratio is dominated not by the physical destruction, but by the cascade term. In the single-day case, hardware replacement accounts for approximately sixteen per cent of the defender's total exposure, the cascade term for the remaining eighty-four per cent. In the three-day case, the hardware share falls to approximately six per cent against a cascade share of ninety-four per cent. This result is robust across the entire published input range: even if UAS unit cost is taken at the upper bound of 50,000 USD and transformer cost at the lower bound of 2 million USD, the cascade term remains dominant. The policy implication is direct and follows from the arithmetic rather than from doctrinal assertion: measures that reduce cascade duration deliver substantially greater economic return than measures that protect individual hardware assets.

5.1.4. Probabilistic Extension: Saturation and Critical Attack Intensity

The deterministic model above assumes that a strike occurs and succeeds. Because saturation tactics are inherently probabilistic, the model is extended to expected values. Let p denote the single-shot probability of kill of the defensive layer against one incoming asset, and n the number of assets committed to the raid. Under the assumption of independent engagements, the probability that at least one asset penetrates the defensive screen is:

$$P_{\text{leak}} = 1 - p^n$$

This expression yields the central quantitative finding regarding the limits of interception. At a single-shot probability of kill of 0.90 against a ten-asset raid, the leakage probability is 0.65; at 0.95 it remains 0.40; and only at 0.99 does it fall below 0.10. Doubling the raid size to twenty assets raises the corresponding values to 0.88, 0.64 and 0.18 respectively. The defensive layer must therefore achieve near-perfect performance to reduce leakage below one in ten, while the attacker requires only an increase in raid size to restore the earlier leakage probability at marginal additional cost. The asymmetry is thus not merely economic but combinatorial.

Expected loss per raid follows directly, distinguishing the unprotected node from the node equipped with the resilience package:

$$\begin{aligned} E[L] &= P_{\text{leak}} \cdot (C_{\text{hardware}} + C_{\text{cascade}}) \\ E[L_{\text{res}}] &= P_{\text{leak}} \cdot (C_{\text{hardware}} + (1 - r) \cdot C_{\text{cascade}}) \end{aligned}$$

where r denotes the cascade reduction factor achieved by the resilience layer at the protected node, that is, the proportion of the macroeconomic outage loss avoided through maintained local supply. Applying the reference values with a single-shot probability of kill of 0.90, a ten-asset raid, a single-day cascade and a cascade reduction factor of 0.90, the expected loss falls from approximately 23.2 million USD per raid at an unprotected node to approximately 5.6 million USD at a protected node, an expected benefit of some 17.6 million USD per raid.

The final step converts this per-raid benefit into a decision threshold expressed in attack frequency. Treating raid arrivals as a stochastic process of intensity λ , measured in raids per year against the protected node, and annualizing the resilience package over its service life T with annual operating expenditure C_{OM} , the critical attack intensity at which the investment breaks even in expected-value terms is:

$$\lambda^* = (C_resilience / T + C_OM) / (P_leak \cdot r \cdot C_cascade)$$

Applying the reference values, with an annualized package cost of approximately 1.16 million USD comprising 0.80 million USD of depreciation over fifteen years and 0.36 million USD of operating expenditure, the critical attack intensity is approximately 0.066 raids per year. Expressed inversely, the investment is justified in expected-value terms if a saturation raid against the protected node is anticipated more frequently than once every fifteen years.

This threshold is the principal quantitative result of the study, and its significance lies in how low it is. A once-in-fifteen-years expectation of a saturation raid against a national transformer station is not a pessimistic assumption under contemporary threat conditions; it is a conservative one. The documented strike frequency in the Ukrainian theater exceeds this threshold by two orders of magnitude, and the emergence of comparable capabilities in the Middle Eastern theater indicates that the relevant intensity for European nodes is no longer negligible. The conclusion is therefore not that resilience investment may be justified under adverse assumptions, but that it is justified under almost any non-zero threat assumption.

The cascade propagation underlying the term $C_cascade$ may be represented formally. Let the transmission network be modelled as a graph $G = (V, E)$, where the vertex set V comprises transformer stations and generation nodes and the edge set E comprises transmission lines. For a given vertex, let $S(v)$ denote the number of vertices losing supply following removal of v and the subsequent redistribution of flows. The structural criticality of a node is then:

$$\kappa(v) = S(v) / |V|$$

Adversary target selection is equivalent to maximizing this criticality measure, which explains the observed preference for high-voltage transformer stations over generation assets: the former exhibit higher criticality per unit of ordnance expended. Conversely, equipping a subset of nodes with the resilience package removes those nodes from the propagation set, yielding a reduced criticality:

$$\kappa'(v) = (S(v) - |I(v)|) / |V|$$

where $I(v)$ denotes the set of resilience-equipped nodes that would otherwise have lost supply following removal of v . The strategic significance of this formulation is that the defender influences the criticality of nodes it does not own and cannot physically protect. Resilience deployment at consumption nodes reduces the value of upstream transmission targets without any intervention at those targets, which is the formal expression of the strategic devaluation argument developed in Subsection 5.4.

5.2. Economic Unsustainability of Air Defense

The depth of the problem is further exacerbated by the disparity in direct engagement costs. A single launch of a modern Integrated Air Defense System (IADS) – such as NASAMS or Patriot batteries, costs significantly more than the OWA (One-Way Attack) UAS it is intended to intercept. Launching a multi-million dollar interceptor against a five-figure drone constitutes a mathematical and economic defeat for the defender, even in the event of a successful kinetic kill.

The 2025 Spanish Blackout and the 2026 Ukrainian theater highlighted the financial impacts of saturation attacks: the adversary uses dozens of cheap drones to deplete the defender's inventory of expensive interceptors. Once these finite stocks are exhausted, the infrastructure remains defenseless. Consequently, the protection of the national power system cannot rely solely on the physical destruction of incoming drones; the defending nation would face financial insolvency long before the attacker exhausted their UAS inventory.

It should be emphasized that this finding does not argue for the abandonment of air defense, which retains its function against manned platforms and cruise missiles. It argues that air defense cannot be the primary economic instrument of transformer station protection, because the exchange ratio is structurally adverse and cannot be improved by procurement volume.

5.3. Contemporary Macroeconomic Challenges

The third dimension of this asymmetry is the macroeconomic damage resulting from supply disruption. As established in previous chapters, the vulnerability of the Electrical Power System (EPS) triggers a systemic domino effect. The cost of a regional blackout caused by a successful drone strike includes not only the replacement of the transformer but also lost industrial output, destroyed digital data, and the massive overhead costs of maintaining social order during the crisis. Economic analyses following the 2025 Spanish Blackout demonstrated that the per-minute damage of a grid collapse exceeded the annual maintenance cost of an entire mobile emergency generator fleet. Based on this realization, a paradigm shift is mandatory: defense expenditures must be measured not against the price of the drones, but against the scale of the avoided economic multiplier damage (Wing et al., 2025).

The cost model presented in Subsection 5.1 permits this paradigm shift to be stated as a decision rule rather than a recommendation. Because the cascade term dominates the defender's exposure by one to two orders of magnitude, the correct denominator for resilience investment appraisal is avoided outage duration, not protected asset value. This reframing is the analytical basis of the break-even calculation that follows.

5.4. Resilience as an Economic Weapon

Against the asymmetry detailed above, only one rational defense exists: the strategic devaluation of the target. By re-engineering the power grid so that the destruction of a single central node does not result in systemic collapse (facilitated by decentralized redundancy), the attacker's strategic advantage is neutralized (ENSEC COE, 2023).

5.4.1. The Resilience Break-Even Point

The resilience package modelled for the reference node comprises four elements: a 20 MWh Battery Energy Storage System providing millisecond-latency stabilization and black-start capability; 10 MW of containerized mobile synchronous generation providing multi-day autonomy; mobile step-up transformation and switching equipment enabling injection into the local medium-voltage network; and the AI-based energy management and segmentation layer described in Subsection 6.3.

Applying published commercial-scale unit costs, the storage element accounts for approximately 5.0 million USD, the generation element for approximately 5.0 million USD, the mobile transformation and switching equipment for approximately 1.5 million USD, and

integration of the management layer for approximately 0.5 million USD, giving a total acquisition cost of approximately 12.0 million USD per protected node, with annual operating and maintenance expenditure of some 3 per cent of capital cost over an assumed fifteen-year service life.

Against the hourly cascade loss derived in Subsection 5.1.2, the Resilience Break-Even Point is reached at approximately ten hours of avoided regional interruption. Expressed differently, the package amortizes within a single working day of prevented outage at one protected node. Since the documented Ukrainian and Iberian events produced interruptions measured in days rather than hours, the investment returns its full acquisition cost on its first successful intervention, and every subsequent hour of maintained supply constitutes net economic gain.

This result inverts the conventional appraisal logic applied to emergency power assets. Standby generation is customarily treated as insurance, a sunk cost justified by low-probability, high-consequence events. The break-even calculation, together with the critical attack intensity derived in Subsection 5.1.4, demonstrates that under contemporary threat conditions, where strike probability against transformer stations is no longer low, decentralized resilience is not insurance but a positive-return infrastructure investment. The distinction matters for procurement: insurance is minimized, whereas positive-return investment is scaled.

5.4.2. Scope and Limitations of the Model

Three limitations must be stated. First, the cascade coefficient is scaled from the regional aggregates of Wing et al. (2025) and does not capture the sectoral composition of any specific Central European load centre; site-specific appraisal would require disaggregated regional input-output data. Second, the critical attack intensity derived in Subsection 5.1.4 is a threshold rather than a forecast: the model establishes the frequency above which investment is justified, but does not estimate the actual frequency, which is a matter for threat assessment rather than economic modelling. Third, interceptor unit costs are open-source estimates and vary by procurement contract; the Interception Economy Index is consequently presented as an order-of-magnitude finding. None of these limitations affects the direction of the results, since all three would have to move by more than an order of magnitude to reverse the sign of the asymmetry.

The establishment of georedundant bases within the framework of national defense is a proactive response to the disproportionately large damages caused by grid-wide darkness. The deployment of decentralized, grid-independent emergency power assets eliminates the attacker's economic leverage. While a drone strike may still cause physical damage, it fails to achieve its strategic objective: the paralysis of the state's operational capability.

5.5. Directed Energy Weapons: Partial Correction of the Interception Economy

The economic asymmetry established in the preceding subsections has not gone unanswered. Since 2024, several states have accelerated the transition of high-energy laser directed energy weapons from experimental status to operational fielding, driven explicitly by the cost-exchange problem quantified above. Two programmes are documented sufficiently to permit analysis.

The United Kingdom's DragonFire programme completed live-fire trials at the Hebrides range in November 2025, engaging drone targets at speeds up to 650 km/h and achieving the first British above-the-horizon tracking and interception of high-speed aerial targets. A 316 million pound production contract was awarded to MBDA UK, with initial fielding on Type 45 destroyers advanced to 2027, five years earlier than originally scheduled. The declared cost per engagement is approximately 10 pounds in electrical energy, against Aster interceptor costs measured in hundreds of thousands of pounds (UK Ministry of Defence, 2025).

Israel's Iron Beam system, delivered to the Israel Defense Forces in operational configuration in December 2025, represents the first high-energy laser worldwide to pass beyond test firings into fielded service. The 100 kW-class system engages rockets, mortars and unmanned systems at ranges up to approximately seven to ten kilometres, at a declared cost of a few dollars per engagement against interceptor costs of 10,000 to 100,000 USD. Critically for the present analysis, lower-powered precursor systems achieved documented combat interceptions of some forty hostile drones in October 2024, and Iron Beam was employed operationally during the Iranian missile and drone attacks of 2025, providing the first operational validation of directed energy defense against precisely the Shahed-class threat examined in Subsection 5.1 (Israeli Ministry of Defence, 2025; Rafael, 2025).

5.5.1. Recomputation of the Interception Economy Index

Applying the directed energy cost per shot to the Interception Economy Index defined in Subsection 5.1.1 produces a decisive change in the engagement economy. Against the reference UAS unit cost of 35,000 USD, a laser engagement at approximately 13 USD yields an index value of roughly four ten-thousandths, compared with the value of twenty-nine derived for a single-shot missile engagement. The improvement is approximately five orders of magnitude. Furthermore, because the directed energy magazine is bounded by generated power rather than by stored munitions, the magazine-depth constraint identified in Subsection 5.2, which rendered the missile exchange terminal rather than merely unfavourable, is removed at the engagement level.

On the engagement metric alone, therefore, directed energy weapons appear to resolve the asymmetry that this study has documented. The following subsection demonstrates that this appearance is misleading, and that the resolution is partial in a manner directly relevant to the protection of transformer stations.

5.5.2. Why the Cost-Exchange Ratio Remains Unchanged

The Interception Economy Index measures marginal engagement cost. It does not measure the defender's total exposure, which the Cost-Exchange Ratio captures. Three factors prevent the directed energy layer from correcting the Cost-Exchange Ratio.

The first is capital cost against coverage geometry. Each laser director is estimated at tens of millions of dollars per unit, with effective engagement radii in the order of seven to ten kilometres. Protecting a national network of several dozen critical transformer stations therefore requires a comparable number of directors, generating an aggregate capital requirement one order of magnitude above the resilience package costed in Subsection 5.4.1. Unlike that package, the directed energy capital expenditure generates no return outside the engagement itself, since it neither shortens outage duration nor produces economic value in peacetime.

The second is residual leakage, and the probabilistic model of Subsection 5.1.4 quantifies it. No interception architecture achieves unity probability of kill, and the cascade term of the Cost-Exchange Ratio is triggered by a single penetration. Even a directed energy layer performing at a single-shot probability of kill of 0.95 leaves a leakage probability of 0.40 against a ten-asset raid. Because the cascade term dominates the defender's exposure by one to two orders of magnitude, the marginal value of raising interception probability from 0.90 to 0.95 is substantially lower than the marginal value of reducing outage duration by a comparable proportion. The arithmetic of the cascade term therefore favors resilience investment over interception investment even where interception has become inexpensive.

The third, and the principal original finding of this study, is the recursive power dependency of directed energy defense. A high-energy laser is an electrically powered system. Its engagement capacity is bounded, as the DragonFire documentation states explicitly, by available power generation and thermal management capacity rather than by ammunition. A directed energy installation defending a transformer station therefore draws its operating power from the electrical network of which that station forms a part. Should the station be neutralized, or should the supplying grid segment collapse, whether through a leaker, a preceding strike, or cascading propagation from an adjacent node, the laser defending it becomes inoperative precisely at the moment of greatest operational need.

This dependency can be stated formally. Where A denotes the availability of the directed energy layer and P_{local} denotes locally available electrical power, then:

$$A_{\text{DEW}} = f(P_{\text{local}})$$

Since P_{local} is the adversary's designated target, the directed energy layer inherits the vulnerability of the very asset it is deployed to protect, unless that dependency is severed by autonomous local generation and storage.

5.5.3. Directed Energy as a Complement Rather than a Substitute

The foregoing analysis yields a conclusion that inverts the intuitive reading of directed energy proliferation. These weapons do not render decentralized energy resilience unnecessary; they make it a precondition. A laser director without local power autonomy is a single-strike asset, whereas a laser director backed by a Battery Energy Storage System and mobile synchronous generation retains engagement capacity through the degradation of the surrounding network.

The resilience architecture proposed in Section 6 therefore occupies a position in the defensive hierarchy that the existing literature has not assigned to it. In the International Energy Agency roadmap (Hart et al., 2025) and in the NATO Energy Security Centre of Excellence assessments (ENSEC COE, 2023), decentralized energy assets are framed as recovery and continuity instruments, that is, measures that mitigate the consequences of a successful strike. The present analysis establishes an additional and prior function: the resilience layer is the enabling infrastructure of the emerging directed energy defensive layer. Under this reading, national investment in mobile generation and industrial storage is not an alternative to participation in the directed energy transition, but its logistical and doctrinal prerequisite.

6. Technological Response Framework

In the era of asymmetric threats, the protection of the national electrical power system can no longer rely solely on the physical interception of offensive assets.

The essence of the strategic response is a paradigm shift from static defensive posturing to functional survivability, or operational resilience. By re-engineering network architecture to maintain critical functions despite the loss of individual nodes, the state neutralizes the strategic leverage sought by the adversary through low-cost attrition.

6.1. Mobile Synchronous Generator Fleets

The primary technological pillar of distributed resilience is the mobile synchronous generator system. Unlike traditional emergency standby units, these assets are capable of phase-accurate synchronization with a degraded or fluctuating grid, or maintaining a stable, fully independent “island mode” operation.

Operational data from the 2026 Middle Eastern UAS strikes confirmed that fixed-site emergency power assets are easily identified and neutralized. In contrast, mobile fleets capable of redeployment within a 6-8 hour window form a dynamic and flexible defensive line. These systems ensure the sustainment of critical infrastructure (hospitals, hardened C2 nodes) even after the total destruction of 750/400 kV primary feed points. Utilizing mobile step-up transformer stations, low-voltage generation can be injected directly into local medium-voltage grids, effectively isolating functional degradation to specific network segments (Hart et al., 2025).

6.2. Industrial BESS: The “Energetic Shield” of the Grid

The second modern component of the technological response is the high-capacity Battery Energy Storage System (BESS). Recent advancements have proven that electrochemical storage is an indispensable tool for in-extremis crisis management.

The decisive advantages of BESS units are millisecond-latency response times and Black Start capability (the ability to re-energize a de-energized grid). During the 2025 Spanish Blackout, it was demonstrated that restarting conventional thermal plants without external voltage is exceptionally difficult; in that theater, decentralized BESS units provided the necessary frequency reference and excitation voltage to the system. These storage assets bridge the critical time gap until mobile generator fleets arrive and reach operational status, thereby preventing systemic frequency collapse.

6.3. Autonomous Grid Management and AI-Enabled C2

Managing a hybrid technological response (BESS + Generators) during the chaotic initial minutes of a large-scale disruption is beyond human cognitive capacity. Consequently, decentralized resilience must be supported by an Artificial Intelligence (AI) platform.

AI-driven control systems can detect physical or cyber-anomalies in real-time. In the 2026 threat environment, AI-enabled algorithms possess the autonomy to segment and isolate critical assets from a compromised national grid and transition them to island-mode operation without human intervention. This technological automation is the only viable method to neutralize grid transients induced by asymmetric UAS strikes before they trigger a nationwide cascading blackout (Directive 2022/2557/EU, 2022).

6.4. The Integrated Hybrid Model

The technological response cannot be reduced to the procurement of individual devices. Its defining characteristic is integration: the four capabilities described in

Subsections 6.1 to 6.3 and in Subsection 5.5 operate on incompatible timescales and address distinct failure modes, and their defensive value arises from the transitions between them rather than from their individual performance. This subsection specifies the architecture of those transitions.

6.4.1. Functional Layers and Their Temporal Domains

The model comprises four layers, each defined by the time window within which it must act.

The electrochemical layer, comprising industrial-scale Battery Energy Storage Systems, occupies the interval from zero to approximately fifteen minutes. Its function is frequency and voltage arrest: the injection of synthetic inertia and reactive support within milliseconds of the disturbance, before the rate of change of frequency crosses the threshold at which protection systems initiate cascading disconnection. This layer also holds the black-start capability required to re-energize a de-energized segment, since conventional thermal generation cannot restart without an external voltage reference, the constraint demonstrated during the 2025 Iberian event.

The rotating layer, comprising containerized mobile synchronous generation, occupies the interval from approximately six hours to indefinite duration. Its function is sustained autonomy: the provision of genuine rotating inertia, short-circuit contribution sufficient for local protection coordination, and multi-day supply to the protected load. Deployment latency of six to eight hours defines the lower bound of this layer's temporal domain, and consequently defines the minimum energy capacity that the electrochemical layer must hold in order to bridge to it.

The cognitive layer, comprising the AI-based energy management and segmentation system, operates continuously and spans all temporal domains. Its function is orchestration: anomaly detection, autonomous decision to segment and island the protected node, sequencing of the electrochemical to rotating handover, load prioritization under constrained supply, and reintegration with the transmission network once external conditions permit. The decision windows involved are measured in tens to hundreds of milliseconds and are therefore beyond human reaction capacity, which establishes automation as a technical necessity rather than an efficiency measure (Kroposki et al., 2023).

The kinetic and directed energy layer, where deployed, operates in the terminal engagement window of seconds. As established in Subsection 5.5, its availability is conditional upon the electrochemical and rotating layers, since a directed energy installation without local power autonomy ceases to function at the moment the network it defends is degraded.

6.4.2. The Critical Handover Sequence

The integration requirement is most clearly expressed through the sequence of events following a successful strike on a transformer station serving a protected node.

At the moment of impact, the protected node loses its primary feed. Within the first cycles, frequency and voltage at the node begin to deviate; the cognitive layer detects the deviation and evaluates whether it originates locally or propagates from the wider network. Within the first hundreds of milliseconds, the cognitive layer executes the segmentation decision, opening the point of common coupling and committing the node to island operation. Simultaneously the electrochemical layer transitions from

grid-following to grid-forming control, establishing the voltage and frequency reference for the islanded segment.

Within the first minute, the cognitive layer sheds non-critical load to bring demand within the sustainable discharge envelope of the storage asset. The load prioritization hierarchy applied at this step follows the healthcare continuity requirements documented by Christián et al. (2025), in which the simultaneous maintenance of clinical function and of inter-organizational communication capability is established as the determining criterion. The practical consequence is that hospital load is prioritized together with the communication infrastructure serving it, rather than clinical load alone, since the findings of that study indicate that clinical continuity without coordination capability does not preserve sectoral function.

Within the first hours, mobile synchronous generation deploys to the node, synchronizes to the island reference established by the storage asset, and assumes the base load; the electrochemical layer reverts to a stabilization and reserve role, recharging from surplus generator output. From that point the node sustains indefinite autonomous operation, subject to fuel resupply, and the directed energy layer, if present, retains full engagement capacity throughout, drawn from the autonomous local supply.

The failure of any single layer degrades but does not defeat this sequence, which is the architectural property that distinguishes the integrated model from the sum of its components. Absence of the electrochemical layer means the node cannot survive the interval before generator arrival, and the sequence fails at the first step regardless of generator capacity. Absence of the rotating layer limits autonomy to the storage duration, converting sustained resilience into delay. Absence of the cognitive layer means the segmentation decision is not taken within the available window, and the node is carried into the cascade with the wider network despite possessing adequate local generation. Absence of the directed energy layer increases strike probability but does not affect post-strike continuity.

6.4.3. Integration with the Cost Model

The four-layer architecture is the physical realization of the Resilience Break-Even Point derived in Subsection 5.4.1. The break-even calculation is valid only if the node in fact sustains supply through the outage, which in turn requires that the handover sequence complete without interruption. The costed package of Subsection 5.4.1, comprising twenty megawatt-hours of storage, ten megawatts of mobile generation, mobile transformation and switching, and the management layer, is therefore not a list of desirable capabilities but the minimum configuration at which the ten-hour break-even result holds.

Partial procurement does not yield proportionally reduced benefit. A node equipped with generation but without storage does not reach break-even at twenty hours instead of ten, but fails to reach it at all, because the sequence terminates at the first handover. This is the sense in which the model is integrated rather than modular, and it carries a direct procurement implication: resilience capability at a protected node is not divisible, and appraisal at the level of individual equipment classes will systematically understate the value of the complete configuration while overstating the value of partial deployments.

6.4.4. Institutional and Human Capital Preconditions

The cost model of Section 5 and the handover architecture specified above share an implicit assumption that requires explicit statement, since it constitutes a binding non-monetized input. Both presuppose competent operation. The Resilience Break-Even Point is realized only if grid-forming inverter control is correctly configured, if the islanding logic is validated against the protection settings of the local network, and if the load prioritization hierarchy has been established in advance in accordance with the sectoral continuity requirements identified in Subsection 6.4.2. A resilience package operated by personnel unable to perform these tasks would not deliver the modelled outcome, and the investment appraisal would be invalid irrespective of the accuracy of its financial inputs.

The competence required is unusual in that it spans domains conventionally separated in professional formation: power system engineering, critical infrastructure protection regulation, and autonomous control system validation. Kátai-Urbán et al. (2025) document that Hungarian higher education and doctoral training in critical infrastructure protection is being continuously developed in direct response to the transposition of the Critical Entities Resilience Directive, and that the curricula are being adapted to the changing legal and security framework. This finding is material to the present study for a specific reason: it establishes that the institutional pipeline for the required interdisciplinary competence exists and is being aligned with the same regulatory instrument that mandates the resilience obligation. The proposed architecture is therefore not constrained by an absent competence base, and the human capital precondition is satisfiable within existing national structures rather than requiring the creation of new ones.

The corollary is that resilience procurement and training capacity must be planned jointly. Equipment deployed faster than the competence to operate it would produce nodes that appear protected in inventory terms while failing at the first handover, which is the most expensive of the possible failure modes because it combines full capital expenditure with zero cascade reduction.

7. Conclusions

Based on the analysis of 21st-century conflict patterns and systemic vulnerabilities, this study concludes that a fundamental paradigm shift is required in the protection of the National Electrical Power System (EPS). Legacy centralized architectures and static defense doctrines have proven obsolete against the economic and operational challenges of modern UAS technology and hybrid warfare. The author contends that the strategic center of gravity for infrastructure defense must shift from geographic borders to decentralized, consumption-centric emergency power nodes capable of autonomous operation.

7.1. Distinction between Synthesis and Original Contribution

The author acknowledges that the individual technological components proposed here are established in the existing literature. Mobile generation and distributed storage for grid resilience are documented in the International Energy Agency's Ukraine roadmap (Hart et al., 2025), and decentralized architecture as a resilience principle is developed in the NATO Energy Security Centre of Excellence assessments (ENSEC COE, 2023; ENSEC COE et al., 2025). The present study does not claim novelty for these components. Its original contributions are analytical rather than technological, and are four in number.

First, the parametric cost model of Subsection 5.1 and the Resilience Break-Even Point derived from it convert the qualitative resilience recommendation into a quantified investment decision rule. The probabilistic extension of Subsection 5.1.4 completes this by deriving a critical attack intensity of approximately one raid per fifteen years, above which the investment is justified in expected-value terms. Together these establish that decentralized resilience is not insurance against a low-probability event but a positive-return investment under contemporary threat conditions, and they identify avoided outage duration rather than protected asset value as the correct appraisal denominator.

Second, the recursive power dependency established in Subsection 5.5.2 identifies a relationship absent from the cited sources. Because directed energy defense is electrically powered, the resilience layer functions not only as a recovery instrument but as the enabling precondition of the emerging directed energy defensive layer. This repositions decentralized energy investment within the defensive hierarchy, from consequence mitigation to capability enablement, and it implies that states pursuing directed energy procurement without a corresponding resilience programme will field a capability that is unavailable under the conditions for which it was acquired.

Third, the handover sequence and layer-failure analysis of Subsection 6.4.2, together with the graph-theoretic criticality formulation of Subsection 5.1.4, establish the non-divisibility of resilience capability at the node level and demonstrate that resilience deployment at consumption nodes reduces the strategic value of upstream transmission targets without any intervention at those targets.

Fourth, the cross-theater validation of Subsection 3.4 elevates the empirical basis of the model from single-theater observation to repeated regularity. The targeting patterns, the distributed damage geometry and the doctrinal transfer documented in the 2026 Middle East escalation replicate the Ukrainian record and, in the dimension of gas-electric coupling, extend it, demonstrating that the identified attrition logic is a property of the adversary doctrine rather than of a particular theater.

Taken together, these four elements constitute the claim of novelty of this study, and the claim is stated explicitly. To the author's knowledge, no previous work has integrated a parametric cost-exchange model of UAS-based attrition, its probabilistic saturation extension, a graph-theoretic formulation of node criticality, the recursive power dependency of directed energy defense, and a two-theater empirical validation drawn from the Ukrainian war and the 2026 Middle East escalation into a single doctrinal decision framework for the protection of national critical electricity infrastructure. The individual instruments exist in separate bodies of literature, in defense economics, in power system engineering and in infrastructure protection doctrine respectively, but their synthesis into one coherent, quantified investment decision rule, culminating in the critical attack intensity threshold of Subsection 5.1.4, has not previously been presented. It is this synthesis, rather than any single component, that the study offers as its contribution to the field: a transferable methodology by which any state operating a centralized transmission system can convert the qualitative imperative of resilience into a quantified, defensible procurement decision.

7.2. The Legal Deficit as a Premise of the Technological Argument

The conclusion of the legal analysis in Subsection 3.5 is a necessary premise of the foregoing and is therefore restated. International Humanitarian Law establishes prohibitions against attacks on objects indispensable to civilian survival, but confers no enforceable protective capability upon the targeted state, and operates on a timescale

wholly unrelated to that of the attack. Where key states have not ratified the relevant Protocol, the residual protection rests on customary law with correspondingly weaker enforcement. The documented targeting of civilian electrical infrastructure in successive theaters confirms that this framework does not deter.

It follows that the legal deficit must be treated as a structural condition rather than as a temporary defect awaiting remedy, and that the compensating capability must be technological and under the exclusive control of the defending state. The architecture proposed in this study is the form that compensation takes: it substitutes autonomous functional survivability for an unenforceable prohibition.

7.3. All-Hazards Applicability and Implementation Pillars

While this research was prioritized by the demands of asymmetric warfare, the proposed technological framework establishes a comprehensive all-hazards capability. The system's mobility, rapid deployment within six to eight hours, and island-mode stability provide a robust defense not only against kinetic strikes but also against extreme climate-driven events and major industrial failures. As evidenced by the 2025 Iberian crisis and by the Middle Eastern escalations, internal stability and Continuity of Government can only be guaranteed through the autonomous defensive architecture proposed here.

Three pillars are defined for strategic implementation. Technological hybridity requires merging mobile synchronous generator fleets with high-capacity Battery Energy Storage Systems to ensure both instantaneous response and sustained operational autonomy, in the non-divisible configuration specified in Subsection 6.4.3. Digital command and AI integration requires the use of artificial intelligence for autonomous anomaly detection and the prevention of cascading systemic failures without human intervention, on the decision timescales established in Subsection 6.4.1 (Kroposki et al., 2023). Geo-redundant posture requires implementing a consumption-centric model that operates independently of traditional grid topology, which is the deployment pattern that yields the criticality reduction formalized in Subsection 5.1.4.

It is recommended that the planned investment framework be treated not as a technical upgrade, but as a vital state risk-mitigation measure, and that its appraisal apply the decision rule derived in Section 5 rather than conventional standby-asset accounting. By acting as a strategic redistributor, the state ensures that the national economy is protected from exponential damages. In the contemporary security environment, national resilience and sovereignty are directly dependent on the continuity of operations of vital systems. Self-determination is maintained only if the grid's functional integrity is guaranteed through these decentralized capabilities, even in the event of total systemic collapse (Hahn et al., 2025).

7.4. Directions for Further Research

Three lines of further work follow from the limitations stated in Subsection 5.4.2. The cascade coefficient requires calibration against disaggregated national input-output data to permit site-specific appraisal of individual load centres. The critical attack intensity derived here is a threshold and not a forecast, and its operational application requires an independent threat-assessment estimate of actual raid frequency against national transformer stations. Finally, the recursive power dependency of directed energy defense established in Subsection 5.5.2 warrants

dedicated engineering study, since the power and thermal management requirements of laser directors under sustained engagement conditions will determine the storage and generation capacity that a co-located resilience package must hold, and those requirements are not yet available in the open literature.

REFERENCES

Al Jazeera. (2026). *Iranians Suffer from Power Blackouts During War and Heatwave*. Al Jazeera, 19 July 2026. Available at: <https://www.aljazeera.com/news/2026/7/19/iranians-suffer-from-power-blackouts-during-war-and-heatwave>.

Anđelković-Lukić, M., & Radović, L. (2024). NATO Attack on FR Yugoslavia in 1999 Was Used to Test the Effectiveness of New Weapons. *Vojnotehnički glasnik / Military Technical Courier*, 72(1), 274-275. Available at: <https://doi.org/10.5937/vojtehg72-37020>.

Castro-Delgado, R., et al. (2025). *Blackout in Spain: Urgent Analysis of Impact on Emergency Medical Services*. *Prehospital and Disaster Medicine*, 1-5. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC12818971/>.

Christián, L., Mészáros, I., Kátai-Urbán, M., Simon, M., Palicz, T., Tiszolczi, B.G., & Tóth, J.J. (2025). The Basis and Practice of Crisis Communication for Critical Health Infrastructure in Selected Institutions of the Hungarian Health Sector. *KOME: An International Journal of Pure Communication Inquiry*, 13(2), 67-94. Available at: <https://folyoirat.ludovika.hu/index.php/kome/article/view/8395/6481>.

Erazo-Chamorro, V.C., Arciniega-Rocha, R.P., Nagy, R., Babos, T., & Szabó, G. (2022). The Prevention of Industrial Security Risk Factors. *Applied Sciences*, 12, Article 10726. Available at: <https://doi.org/10.3390/app122110726>.

Garcia-Sanz, M., Marden, M., Cvetkovic, I., Oh, H., LoCicero, E., & Khalid, S. (2025). Grid Fragility, Blackouts, and Control Co-Design Solutions. *Advanced Control for Applications*, 7(3), e70022, 8. Available at: <https://onlinelibrary.wiley.com/doi/10.1002/adc2.70022>.

Glosson, B.S. (1993). Impact of Precision Weapons on Strategic Air Operations. *Airpower Journal*, 7(2), 4-10. Available at: https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-07_Issue-1-.

Hahn, E., Warner, G., & Gohardani, N. (2025). Enhancing Energy Resilience in Navy Region Southwest: Bridging Capability and Capacity Gaps with Modern Technologies and Utility Acquisition Approaches. In: *Proceedings of the Twenty-Second Annual Acquisition Research Symposium and Innovation Summit*, p. 279. Available at: <https://dair.nps.edu/handle/123456789/5429>.

Hart, C., Vatman, T., & Gebhardt, T. (2025). *Empowering Ukraine Through a Decentralised Electricity System: A Roadmap for Ukraine's Increased Use of Distributed Energy Resources towards 2030*. Paris: International Energy Agency (IEA), Revised Version, February 2025, p. 20. Available at: <https://www.iea.org/reports/empowering-ukraine-through-a-decentralised-electricity-system>.

Human Rights Watch. (2026). *Israel, Iran: Unlawful March Attacks on Energy Infrastructure*. New York: Human Rights Watch, 22 April 2026. Available at: <https://www.hrw.org/news/2026/04/22/israel-iran-unlawful-march-attacks-on-energy-infrastructure>.

International Energy Agency (IEA). (2024). *Ukraine's Energy Security and the Coming Winter*. Paris: International Energy Agency. Available at: <https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter>.

Iran International. (2026). *War Damage Adds New Strain to Iran's Blackout-Prone Power Grid*. Iran International, 11 June 2026. Available at: <https://www.iranintl.com/en/202606115946>.

Israeli Ministry of Defence. (2025). *Delivery of the First Operational Iron Beam High-Power Laser Air Defence System to the Israel Defense Forces*. Tel Aviv: Directorate of Defense Research and Development. Available at: <https://www.jpost.com/defense-and-tech/article-881595>.

Kátai-Urbán, L., Bleszity, J., & Vass, Gy. (2025). A kritikus infrastruktúra védelmi felsőoktatási tapasztalatok a kritikus szervezetek ellenállóképességéről szóló szabályozás tükrében. *Polgári Védelmi Szemle*, 17(Különszám), 220-236. Available at: https://mpvsz.hu/pv_szemlek/pvszemle2025/index.html?search=A+kritikus+infrastrukt%C3%BAra+v%C3%A9delmi+fels%C5%91oktat%C3%A1si+tapasztalato.

Kovács, F. (2024). The Strategic Role of Critical Infrastructure in the Russo-Ukrainian War. *Hadtudomány. Military Science*, 34(3), 29. Available at: <https://real.mtak.hu/227778/1/75113-1-10-20250302.pdf>.

Kroposki, B., Bernstein, A., King, J., Vaidhynathan, D., Zhou, X., & Chang, C.-Y. (2023). Autonomous Energy Grids: Controlling the Future Grid With Large Amounts of Distributed Energy Resources. *IEEE Power and Energy Magazine*, 21(2). Available at: <https://ieeexplore.ieee.org/abstract/document/10083083>.

NATO Energy Security Centre of Excellence (ENSEC COE). (2023). *Resilience of Energy Infrastructure: Strategic Challenges and Technological Solutions*. NATO ENSEC COE Reports. Available at: <https://enseccoe.org/publications/resilience-of-energy-infrastructure/>.

NATO Energy Security Centre of Excellence (ENSEC COE), Bermúdez Fernández, E., & Paksius, J. (2025). *Critical Energy Infrastructure: The Case for Increased Civil-Military Cooperation*. *Energy Highlights*, 20. Available at: <https://www.enseccoe.org/publications/energy-highlights-20/>.

Official Journal of the European Union. (2022). *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC*. Article 6. Available at: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>.

PBS News. (2026). *Iran Intensifies Attacks on Gulf Energy Sites after Israel Struck Its Key Gas Field*. PBS NewsHour, 19 March 2026. Available at: <https://www.pbs.org/newshour/world/iran-intensifies-attacks-on-gulf-energy-sites-after-israel-struck-its-key-gas-field>.

Rafael Advanced Defense Systems. (2025). *Iron Beam High-Energy Laser Air Defence System: Operational Configuration*. Haifa: Rafael. Available at: <https://www.flightglobal.com/military-uavs/rafaels-iron-beam-laser-air-defence-system-enters-operational-service-in-israel/166193.article>.

The Jerusalem Post. (2026). *Ukraine: Russia Providing Iran with Israeli Energy Grid Targets*. The Jerusalem Post, 7 April 2026. Available at: <https://www.jpost.com/middle-east/iran-news/article-892256>.

The Times of Israel. (2026). *Iran Appears to Target Israeli Power Plant in Missile Attack, but Misses*. The Times of Israel, 25 March 2026. Available at: <https://www.timesofisrael.com/iran-appears-to-target-israeli-power-plant-in-missile-attack-but-misses/>.

UK Ministry of Defence. (2025). *Boost for Armed Forces as New Laser Weapon Takes Down High-Speed Drones*. London: Defence Equipment and Support. Available at: <https://des.mod.uk/boost-for-armed-forces-as-new-laser-weapon-takes-down-high-speed-drones>.

United Nations Economic Commission for Europe (UNECE). (2015). *Convention on the Transboundary Effects of Industrial Accidents – As Amended on 15 December 2015*. Annex IV: Preventive Measures Pursuant to Article 6. Available at: <https://unece.org/info/Environment-Policy/Industrial-accidents/pub/21645>.

Varga, F. (2011). The Work and Experiences of the Operational Staff of the Red Sludge Disaster. *Hadmérnök/ Military Engineer*, 6(2), 253-264. Available at: http://hadmernok.hu/112_01_vargaf.pdf.

Wing, I.S., Larsen, P.H., Carvallo, J.P., Sanstad, A., Wei, D., Rose, A., et al. (2025). A Method to Estimate the Economy-Wide Consequences of Widespread, Long Duration Electric Power Interruptions. *Nature Communications*, 16, Article 3335, 1-13. Available at: <https://www.nature.com/articles/s41467-025-58537-4>.

Zampranha, D., & Albuquerque, A. (2024). Cheaper Precision Weapons: An Exploratory Study about the HESA Shahed 136. *Advances in Aerospace Science and Technology*, 9, 40-59. Available at: <https://www.scirp.org/journal/paperinformation?paperid=131823>.