



INTERNATIONAL
RENAISSANCE
FOUNDATION



Holding the Grid: Ukraine's Energy Resilience Playbook



This material was prepared by DIXI GROUP NGO with support of the International Renaissance Foundation within the framework of the project “Strengthening Ukraine’s Resilience in Energy”. The material reflects the views of the authors and does not necessarily represent the position of the International Renaissance Foundation.

© DIXI GROUP, 2026

CONTENTS

Executive Summary	4
Part I: The Threat — How Attacks Evolved (2022–2026)	7
Part II: The Plays — 11 Principles for Energy Resilience	10
Play 1: Reduce Strategic Dependence on Centralised Generation	10
Play 2: Protect and Expand Flexible Generation	12
Play 3: Prioritise Grid Resilience to Ensure Generation Capacity Use	14
Play 4: Consider Cascading Dependencies in Urban Energy Systems as a Distinct Risk	15
Play 5: Ensure Interconnectivity as a Strategic Resilience Factor, but Account for Constraints	18
Play 6: Standardise Equipment and Repair Approaches to Accelerate Recovery	21
Play 7: Integrate Air Defence, Physical (Engineering) and Cyber Protection into Energy Security Planning	22
Play 8: Build Logistics Resilience, Reserves, and Clear Prioritisation for Supplying Primary Energy Sources	27
Play 9: Strengthen Crisis Communications and Grassroot Preparedness	28
Play 10: Enable Industrial Adaptation through Backup Supply and Energy Management	30
Play 11: Use Regulatory Policy to Accelerate Reconstruction and Restore Market Stability	31
Part III: The Agenda — From Wartime Adaptation to Resilience by Design	33

EXECUTIVE SUMMARY

Since February 2022, Ukraine's energy sector has operated under sustained missile and UAV strikes that evolved from early attacks on fuel logistics and large generation assets to repeated, combined campaigns against generation, transmission corridors, distribution networks, and — from 2025 onwards — gas infrastructure and district heating systems. Over time, the threat intensified not only in scale but in frequency, targeting logic, and complexity: attack campaigns increasingly combined different weapon types, repeated strikes on previously damaged facilities, and deliberately targeted both generation capacity and network bottlenecks. This reduced recovery windows, increased operational uncertainty, and shifted the challenge from managing isolated incidents to absorbing and recovering from cumulative damage.

Under these conditions, the concept of energy security has shifted from a narrow capacity-demand question to a broader set of operational capabilities: keeping critical services running under attack, preserving system controllability, and restoring supply rapidly under conditions of repeated damage and equipment scarcity.

Ukraine's pre-war infrastructure legacy was the critical structural constraint throughout. A significant share of key equipment in generation and transmission was designed and operated since Soviet times — with limited replacement options, long manufacturing lead times for compatible hardware, and complex international sourcing requirements. These constraints were compounded by wartime operating conditions: risks to repair crews, restricted site access, repeated air alerts, and the need to prioritise limited materials and technical teams across multiple regions simultaneously.

This paper draws on Ukraine's wartime energy operations from 2022 to early 2026 to identify ten operational lessons and their practical implications for resilience-by-design in infrastructure planning, investment, operations, and governance.

Centralised generation concentrates systemic risk. Systems built around large plants and long transmission corridors create a small number of high-impact nodes. Striking those nodes produces disproportionate disruption and regional supply asymmetry — even when generation capacity remains available elsewhere in the system. The practical implication is not to abandon large-scale generation, but to complement it with distributed capacity for critical loads, modular deployable solutions, and a planning metric of regional adequacy that explicitly accounts for transmission constraints.

Flexible generation is both the backbone of system balancing and the highest-value target. Real-time system stability depends less on total installed capacity than on fast-responding resources that cover peaks, provide reserves, and maintain frequency and voltage under stressed conditions. Because flexible capacity is scarcer and harder to restore, its loss produces a disproportionately large systemic effect — and where flexibility is tied to cogeneration plants, strikes simultaneously undermine electrical manoeuvring capacity and urban heat supply.

Grid resilience determines whether generation capacity can be used. In multiple attack episodes, it was grid assets — substations, transmission lines, distribution nodes — rather than generation that became the binding constraint on supply. High installed capacity

provides no resilience benefit if the grid cannot deliver power, re-route flows around damaged sections, or operate in emergency configurations. Redundancy, sectionalization, and standardised fast-deployable restoration solutions are the operational foundation of grid resilience.

Under sustained attack, urban energy systems shift from reliability optimization to controlled systemic degradation. This is a qualitatively distinct risk type that sector-by-sector resilience frameworks do not capture. Electricity supply disruption functions as a trigger for cascading failures across heating, water, transport, and essential services — and seasonal stress compresses the time window between a manageable deficit and irreversible physical damage. Kyiv's winter of 2025–2026 demonstrated that below a certain threshold, restoring power restores services; above it, damage to pipes, generators, and aging infrastructure accumulates faster than it can be repaired. Planning frameworks must map cross-sector dependency chains, define thresholds of irreversibility for each dependent system, and treat centralised urban heat sources as dual-priority assets.

ENTSO-E synchronisation is a strategic resilience asset, but its value depends on constraints that must be explicitly managed. Cross-border transfer capacity limits, the number and availability of import entry points, internal west-to-east transmission corridors, and system controllability under stressed conditions all determine how much external support can be converted into effective supply where shortages are greatest. Integration should be treated not as an unlimited substitute for domestic resilience, but as a critical asset whose value depends on the condition of the system receiving the support.

Restoration speed depends on standardisation more than on funding. The availability of standardised repair packages, interoperable specifications, mobile substations, and plug-and-play solutions consistently proved more decisive for recovery timelines than the volume of financial assistance alone. A unified nomenclature of critical spare parts, pre-positioned warehouse hubs, and standardised temporary supply configurations reduce restoration time from weeks to days and make international assistance deployable at scale.

Energy security under sustained attack requires layered physical, air defence, and cyber protection — embedded by design, not added after the fact. Air defence reduces the probability and scale of damage; passive engineering protection reduces consequences when strikes penetrate; and cyber protection preserves operational control of assets. Protection must be integrated into modernisation and repair programmes from the outset — as a standard cost of investment, not an optional supplement. Wartime experience shows that facilities degrade faster than they can be restored when protection is absent; the «protection-by-design» principle directly addresses this dynamic.

Oil and gas supply resilience requires distributed storage, clear prioritisation rules, and maintained import capacity. Early attacks on refineries and logistics nodes demonstrated the fragility of supply chains built around centralised storage. The government's rapid pivot to import-based supply — supported by fiscal adjustments, price deregulation, and simplified import procedures — stabilised markets, but also exposed the absence of minimum stock frameworks that would have provided an earlier buffer. For gas, formalised prioritisation through PSO regimes and protected consumer categories provided a more structured response, and this model warrants systematic application to oil products as well.

Crisis communication is an operational function of the energy system, not only a public information task. Effective communication shapes demand behaviour, reduces peak loads, and directly affects system balance during shortage periods. The critical lesson is the systematic differentiation between scheduled outages and emergency restrictions — and the clear, multi-level messaging architecture that makes this distinction actionable for consumers. Equally important is the resilience of communication against deliberate disinformation: in Ukraine's experience, Russian information actors exploited outages to spread panic, trigger destabilising consumer behaviour, and erode trust in operators. This makes message synchronisation across institutions and proactive counter-narrative guidance a structural requirement of crisis communication systems.

Industrial demand response is an underutilised resilience resource. Energy-intensive industries that shifted from compensating outages to actively managing their internal consumption regime — rescheduling loads, deploying short-horizon buffers, improving power quality, and adopting microgrid logic — reduced both their own operational losses and the depth of system-wide restrictions. This transformation converts industry from a passive victim of outages into an active participant in system balancing, and warrants explicit recognition and support in regulatory frameworks.

Regulatory policy is a resilience instrument that operates on two parallel tracks. Wartime fast-track mechanisms — declarative permitting, simplified procurement, emergency contracting — reduce the procedural friction that slows recovery under time pressure. Simultaneously, market stabilisation measures — price caps, liquidity support, non-market procurement for scarce equipment — preserve the financial viability of the actors on whom recovery depends. Neither track is sufficient without the other: procedural speed without financial stability does not produce reliable supply, and financial stability without procedural flexibility does not produce timely restoration.

Ukraine's experience demonstrates that energy resilience is not a property of any single asset or system — it is produced by a portfolio of capabilities that must function simultaneously and reinforce each other: distributed and flexible generation, robust and repairable grids, standardised recovery logistics, layered protection, cross-sector urban planning, disciplined communication, demand-side adaptability, and regulation that removes friction without removing accountability. Institutionalising these capabilities means shifting from ad-hoc emergency response to a durable resilience-by-design model embedded in infrastructure planning, investment decisions, and governance frameworks.

PART I:

THE THREAT — HOW ATTACKS EVOLVED (2022–2026)

After the failure of the initial Russia’s plan of rapid capture (‘blitzkrieg’ or, as per Russian propaganda, ‘special military operation’), Ukraine’s energy infrastructure became a deliberate target. The purpose of aerial strikes (UAVs and missiles) was not only to temporarily disable generation and transmission capacity, but also to strategically undermine the government’s ability to provide critical services (electricity and fuel supply, district heating, water supply, healthcare and other services), to create systemic disruptions in the operation of critical infrastructure, and to increase moral and political pressure on the population and the authorities. Frontline areas are particularly sensitive, where the systematic nature of strikes with shorter-range weapons had a pronounced humanitarian impact. The systematic nature of these actions was frequently used to refer to the very [definition of genocide](#), in particular ‘[d]eliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part’.

The tactics and approaches used to attack the energy sector changed substantially several times throughout the four years of full-scale war; therefore, they can be divided into distinct phases.

PHASE 1 (*February – September 2022*):

fuel logistics and the capture/neutralization of large TPPs

In the first months of the full-scale invasion, the main focus was on the motor fuels sector (refineries, oil depots, pipelines) and large thermal power plants in areas of military advancement. The objective was to rapidly undermine fuel security for both civilian and defense needs; strikes on key capacities (including the Kremenchuk refinery) caused temporary shortages and logistical disruptions.

At the same time, some large thermal power plants found themselves under occupation and/or in active combat zones. Suspension of their operation or loss of dispatch control increased power system risks and reduced available capacities.

PHASE 2 (*October 2022 – March 2023*):

“energy terror” and massive, coordinated strikes on the power system

After setbacks on the battlefield, with Ukrainian forces large-scale offensive in the Kharkiv region (September 2022) and the liberation of Kherson (November 2022), Russia shifted to massive, coordinated strikes against key nodes of the power system targeting primarily transmission (substations and grid nodes), as well as elements of generation – aiming to disable a large number of facilities across multiple regions simultaneously, create large-scale outages, and complicate rapid recovery by targeting “bottlenecks”.

The culmination of this approach was the near-total loss of electricity supply (a large-scale system disintegration leading to blackout) on [November 23, 2022](#), which demonstrated the critical importance of substations for the grid integrity as well as rapid restoration

capabilities. The consequences of attacks during this period by type of facilities are outlined in the [Update on the Energy Damage Assessment \(June 2023\)](#) by UNDP.

PHASE 3 (*April 2023 – February 2024*):

technological “scaling-up” and the combination of weapons applied

In 2023, a trend emerged towards combining different types of weapons (mixing cruise and ballistic missiles of various classes), which complicated air defense and increased requirements for the energy sector’s adaptation. At the same time, the scale of continuous massive strike waves, characteristic of autumn 2022 - early 2023, decreased during certain periods.

A separate systemic shock to water-and-energy infrastructure was [the destruction of the Kakhovka HPP dam \(June 2023\)](#). Despite the facility was not operational due to Russian occupation, its destruction generated significant cross-sectoral impacts: from challenges in cooling power plants in the surrounding areas to lack of water resources for several urban centres and agriculture.

PHASE 4 (*March – December 2024*):

the growing role of UAVs and a campaign against thermal and hydropower generation

From March 2024, an aggressive campaign of strikes on generation facilities was recorded – primarily thermal (coal/gas-fired) and hydropower – alongside an increased use of enhanced UAVs. Strikes were carried out against hydropower and thermal power facilities, including the [Dnipro HPP \(March 2024\)](#) and the [Trypilka TPP \(April 2024\)](#).

As a result of this campaign, [around 10 GW of installed capacity was destroyed or damaged](#), and the power system operator with DSOs widely applied emergency/forced outage schedules to shed demand. Some capacity was restored before winter, and although strike waves continued in autumn - winter 2024, they proved less effective – allowing Ukraine to avoid major blackouts during the winter of 2024-2025.

PHASE 5 (*January – September 2025*):

a shift in focus to gas infrastructure

From early 2025, a new priority became visible: shifting the focus from electricity assets to the gas value chain (production, storage, transmission and related infrastructure). This might be explained by the fact that, despite the 2022-2024 strikes, the power system remained functional and improved its resilience through adaptation, rapid repairs, international support with equipment, and strengthened protection measures. In addition, gas storages in early 2025 were depleted, necessitating increased reliance on domestic production and imports to refill stocks.

Gas is a critical fuel for district heating, part of TPP/CHP generation, and industry; therefore, attacks on the gas infrastructure directly affect the resilience of energy supply during the heating season and also have a significant financial and economic dimension. After some attacks in 2025, a substantial share of daily production was temporarily lost (government estimates: [up to 40–50% in the short term](#)), increasing risks for balance in underground gas storage facilities and preparedness for the winter season.

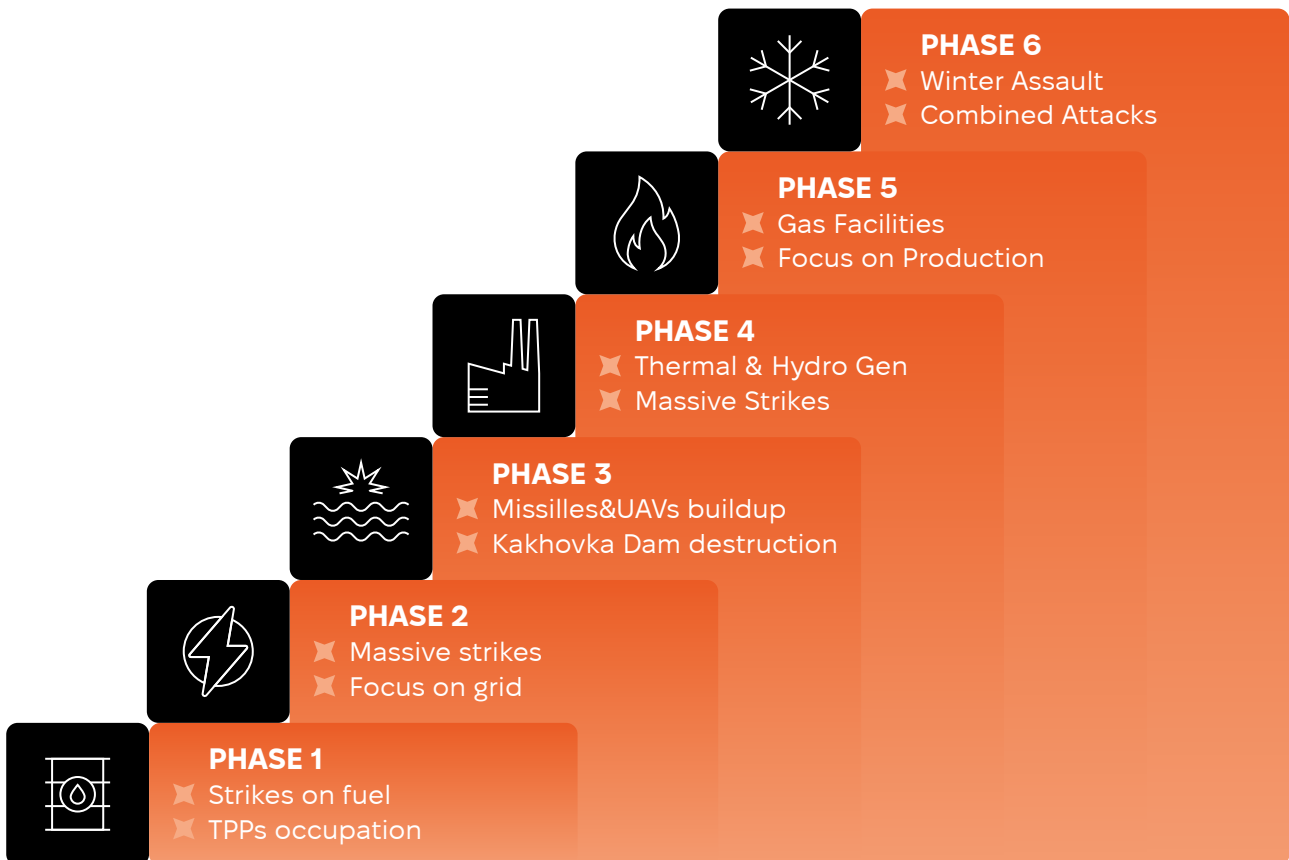
PHASE 6 (October 2025 – February 2026):
transition to a “winter combined campaign”

Starting in October 2025, attacks entered a high-intensity “winter mode,” with [strikes on the gas value chain](#) overlapping with [strikes on electricity system \(substations, power generation\)](#) and [large cogeneration assets critical for district heating](#). This combination, under conditions of peak seasonal demand, creates cascading effects: even local grid damage can produce a tangible impact for large metropolitan areas (emergency/forced outages, changes in operating modes for critical services, increased reliance on backup supply schemes).

Continued attacks on gas producing infrastructure are viewed as strikes on the source of primary fuel of the district heating systems, while parallel pressure on heat generation (CHPs/boiler houses) quickly translates into critical consequences for urban communities.

From a systemic perspective, this marks a shift from the model “strike - capacity deficit” to the model “strike - critical urban impact,” where air defense capabilities, the speed of emergency restoration works, the availability of equipment for such repairs, and backup configurations for supply become decisive factors to avoid infrastructural collapse.

Phases of Attacks on Ukraine’s Energy Sector



PART II:

THE PLAYS — 11 PRINCIPLES FOR ENERGY RESILIENCE

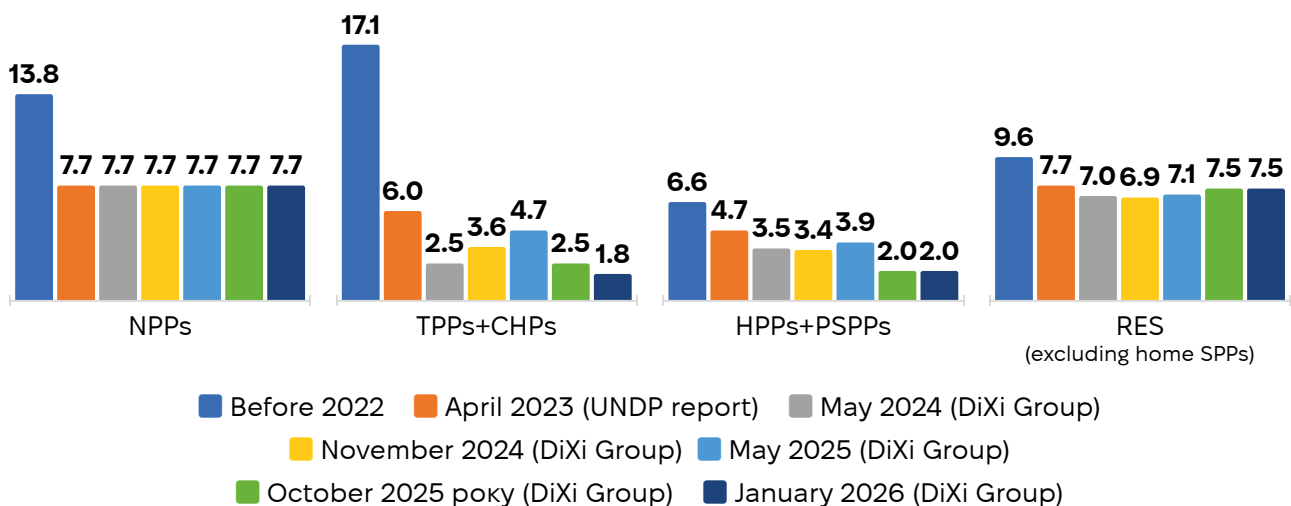
Play 1:

Reduce Strategic Dependence on Centralised Generation

The war experience of Ukraine has shown that a centralized model of energy system that relies critically on large power plants and interregional high-voltage power flows becomes a strategic vulnerability. In such systems, the weak point is not only individual generating units but the entire logic of supply: when large-scale generation and long transmission corridors create a limited number of nodes, striking which produces a disproportionately large systemic effect.

Across all phases of the war, it is clearly observable that large power plants became priority targets. In particular, [in spring 2024 coordinated strikes destroyed more than 9 GW of available generation](#); and in the [massive attack of February 3, 2026](#), TPPs and CHPs in Ukraine's major cities were targeted. A number of large thermal power plants in the east of Ukraine ended up under occupation and/or in active combat zones, namely Luhansk TPP (1,450 MW), Vuhlehirska TPP (3,600 MW), and Myronivska TPP (275 MW). This immediately reduced available resources and increased risks for regional grid stability.

Available generating capacity, GW



The next vulnerability of centralized systems is that they create regional energy dependencies, and interregional power flows become critical. Even if sufficient generation exists at the system level, local deficits may emerge if electricity transmission depends on a limited number of nodes/corridors that can be damaged or congested.

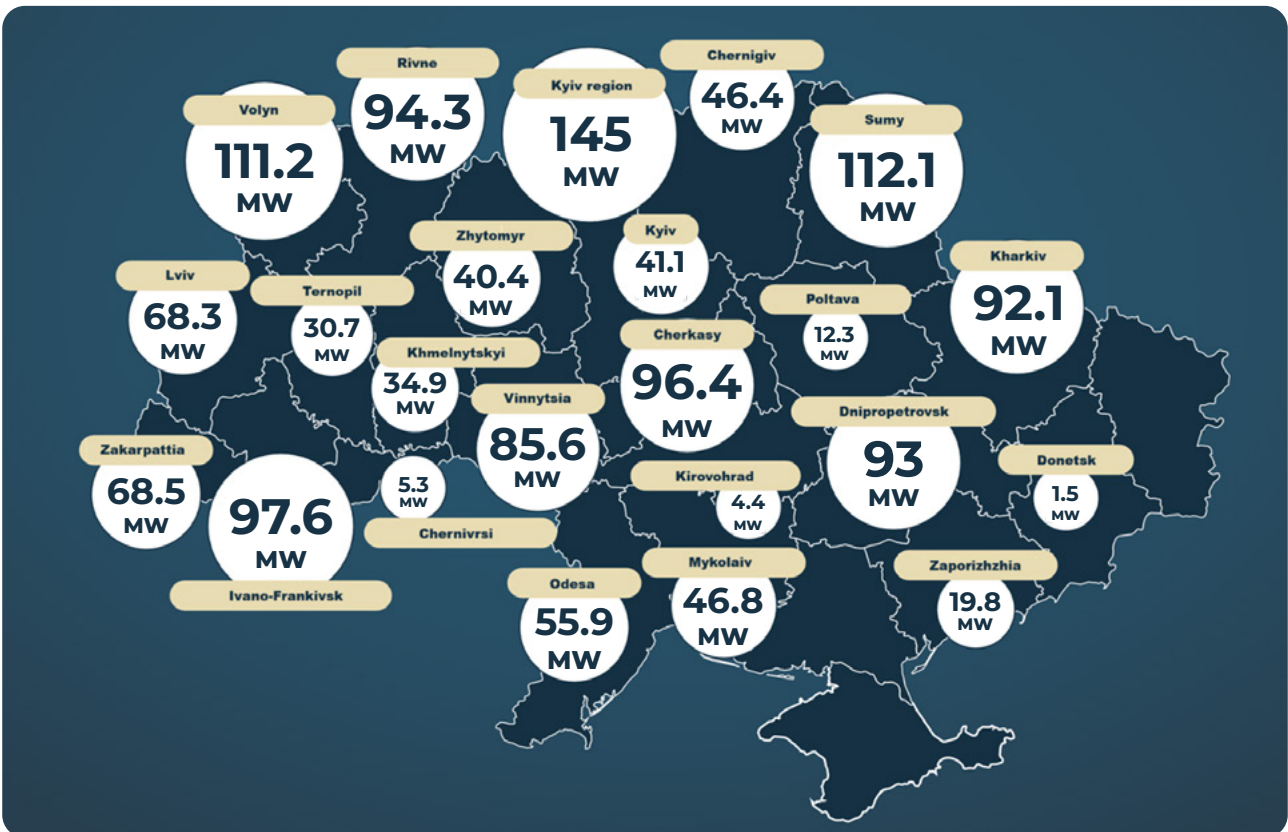
A separate challenge is observed in frontline regions, where “scorched earth” tactics are applied with continuous shelling and relatively slower repairs due to safety risks. For

centralized generation, this creates an additional risk: even when an asset is repairable, the actual repair “windows” (suitable time periods), issues of site access, staff safety, and equipment logistics can significantly constrain restoration speed.

Another effect is the growing difference between regions with a generation surplus (west of Ukraine) and regions with a deficit (east and south of Ukraine) with limited transmission capacity constraining redistribution of electricity. This is a critical “architecture lesson”: centralization makes the system dependent not only on power plants but also on the ability to deliver electricity to end-consumers. Combined damage to generation and transmission amplifies regional asymmetry and makes local outages more likely.

Ukraine is actively expanding its fleet of gas turbine, gas engine and cogeneration units, as a means to strengthen energy resilience and reduce reliance on centralized sources. These assets are designed to meet the needs of communities, critical infrastructure, and industry, enabling relatively rapid capacity deployment and greater operational flexibility of the power system. In the medium term, this distributed generation can serve not only as a backup source but also as a full-fledged market participant, enhancing system balancing reliability and improving the economic efficiency of operation.

Development of Distributed Generation in Ukraine (as of February 2026)



Source: [Ministry of Energy of Ukraine](#)

This lesson does not imply abandoning large power plants as such. Rather, it indicates that relying exclusively on centralized generation and backbone transmission under repeated attacks creates an unacceptable level of systemic risk.

Practical implications for public policy and investment planning:

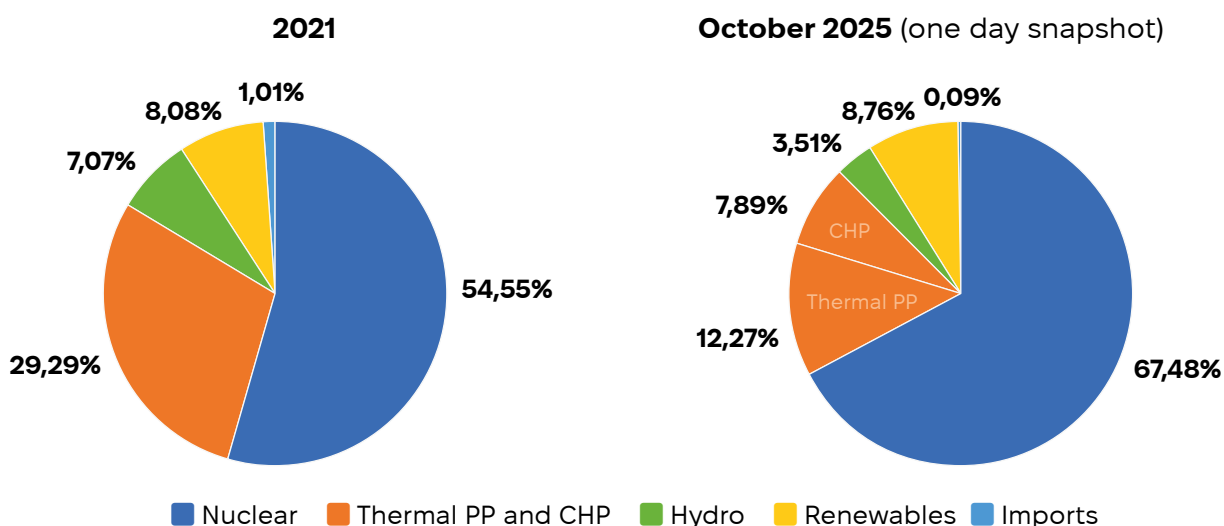
- **Prioritize distributed generation for critical loads** (water utilities, hospitals, district-heating assets, communications, municipal services) as a way to reduce single points of failure – especially in regions at risk of shortages. The logic of “bringing generation closer to the consumer” directly follows from the dependence on vulnerable transmission corridors. Critical infrastructure facilities can also benefit from prosumer models.
- **Modularity and scalability:** support solutions that can be deployed quickly (small gas/diesel units, PV + storage, mobile/modular units) as a tool to rapidly compensate for part of the losses/unavailability of large units and reduce grid overloads.
- **Scale up gas-fired distributed generation (gas-turbine, gas-piston, and cogeneration installations) as a resilience asset:** deploy fast, flexible units for municipalities, critical infrastructure and industry, and in the medium term enable them to operate beyond standby mode by participating in power and balancing/ancillary services markets, improving system reliability and economics.
- **Regional self-sufficiency as a resilience criterion:** in system development planning, introduce a metric of ‘regional adequacy’ (i.e. how much load a region/area can cover locally under network constraints), taking into account the risk of shortages in areas of most probable military impact and transmission limitations.
- **Link to the grid:** improving the resilience of centralized generation is impossible without parallel strengthening of grid reparability and redundancy of key transmission nodes/corridors, as these elements are what “turn” generation losses into regional blackouts.

Play 2:

Protect and Expand Flexible Generation

Ukraine’s wartime experience has clearly shown that the critical property of a power system is not so much the volume of available baseload generation, but rather the presence of flexible resources capable of rapidly changing output and supporting system operation in real time. Flexible generation effectively serves as the “backbone” of balancing: it covers peak demand, compensates for sudden losses of individual system elements, provides reserves, supports frequency and voltage, and enables operators to maintain control under conditions of network damage and unstable loads.

Electricity Generation Mix: 2021 vs October 2025



Source: [ExPro Consulting](#) and [DiXi Group](#) data

Flexible generation facilities perform three key functions which prevent the system quickly shifting from 'deficit' to 'loss of control' in a crisis:

- 1. Peak demand coverage and smoothing of daily fluctuations.** The real 'cost' of a flexibility deficit becomes evident precisely during peak hours: even if energy is sufficient on an average daily basis, a lack of fast-response capacities leads to the need for load shedding or costly imports.
- 2. Operating reserves and frequency control.** Damage to network elements and unpredictable deviations in demand/supply require immediate response. Flexible capacities are the basis for primary/secondary reserves and emergency dispatch.
- 3. Control during repairs and switching operations.** In wartime conditions, the power system constantly operates in emergency configurations: supply schemes change, temporary restrictions are introduced, the number of switching operations increases, and "bottlenecks" multiply. Flexible generation allows operators to 'support' the system adequacy and integrity during such reconfigurations.

However, [flexible generation is a highly efficient target for the adversary](#) because its loss produces a disproportionately large systemic effect. First, flexible capacities are typically smaller in total available volume than baseload ones, and their restoration is often more difficult (specific equipment, limited repair 'windows', fuel dependency, and reliance on robust network infrastructure). Second, attacks on flexible capacities directly undermine the system's ability to maintain balance during critical hours, quickly translating into load shedding by consumption restrictions. Third, part of flexible capacities, as in the case of Ukraine, consists of cogeneration plants, damage to which creates an additional 'dual' effect: a loss of major source for urban district heating. Overall, the logic of attacking flexible generation aims not only to reduce available capacities, but to undermine operational control – so that the system cannot pass the demand peaks normally, maintain reserves, and stabilize after damage.

From a practical standpoint, a flexibility deficit manifests in several major effects. The first is an increase in the frequency and depth of load shedding. When flexible capacities are insufficient, even minor additional disruptions (repairs, local incidents, weather impacts) can push the system into a mode where consumers' outages become the only balancing instrument. Another effect is increased sensitivity to network constraints. With a lack of flexibility, the system's ability to cover deficit through power flows or changes in generation dispatch decreases, which amplifies local deficits and complicates recovery after damage. In cogeneration, there is an effect that has already become [visible even in Ukraine's capital](#): growing risks to urban communities due to the role of CHPs in district heating. For large cities, disruptions at large thermal inputs mean a direct risk to heat supply during peak winter periods.

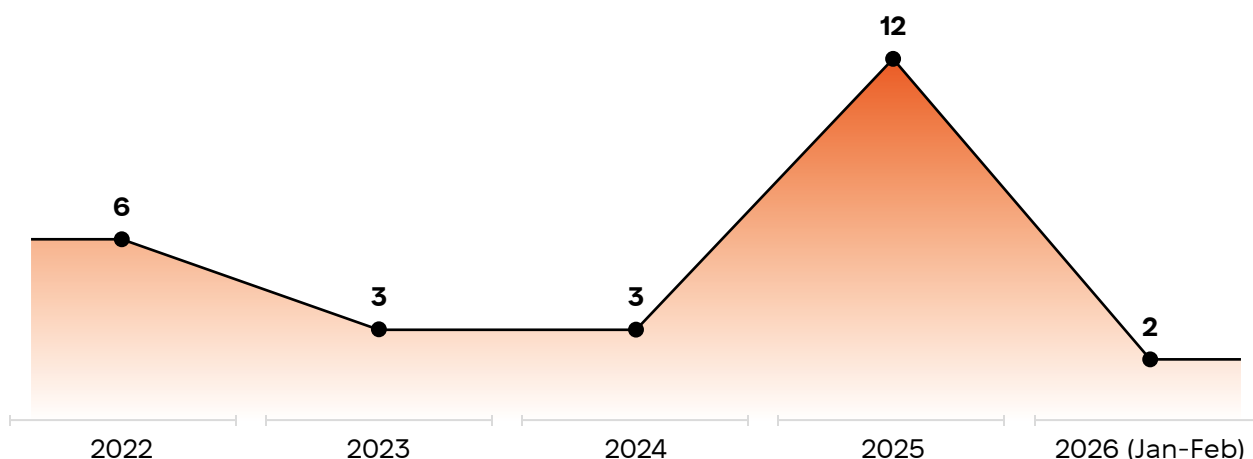
Play 3:

Prioritise Grid Resilience to Ensure Generation Capacity Use

Ukraine's wartime experience has shown that mere surplus in installed capacity over demand does not guarantee reliability: even if generation is available, electricity supply can be disrupted by damage to substations, grid nodes, and transmission lines. In many episodes, it was precisely grid assets (transmission and distribution) that became bottlenecks, creating deficit areas regardless of whether generation existed in the system.

During attacks, what proved critical was not only the ability to produce electricity, but also the system's ability to reconfigure its operation: reroute power flows around damaged sections, quickly isolate faulted segments, and restore connections between demand areas and available generation sources. In simple terms, resilience was determined by whether the power system could remain operational in a "cut-up" mode – through backup lines, alternative routing, and simplified emergency configurations.

Number of mentions on NPPs capacity reductions



Source: DiXi Group, based on the IAEA reports (iaea.org)

A telling case is the Russian winter combined campaign (Phase 6), when damage specifically to transmission assets (especially 330-750 kV substations) caused large-scale outages in Kyiv and the surrounding region: according to official data, on the morning after the January

9, 2026, attack [more than 500,000 consumers were left without electricity](#), and due to network damage emergency and hourly outage schedules were applied in different parts of the city.

Under conditions of systemic damage to transmission and distribution networks, supply disruption works not only through a 'major accident', but also through the accumulation of many local damages that break grid connectivity (island modes/segmentation), congest alternative corridors, increase the number of switching operations, emergency schemes and temporary restrictions, and slow down the normalization of system operation even after generation capacity is restored or reconnected. It is also important that outages in distribution systems (especially in large cities) immediately undermine operations of water utilities, district heating enterprises, operators of critical services and communications – even if the backbone (high-voltage) level is broadly stabilized.

Grid resilience determines both the scale and the speed of recovery: supply can be restored relatively fast through switching/bypass schemes and later returned from emergency configurations to normal ones once the system elements are restored. In practice, this boils down to three groups of capabilities:

- 1. Redundancy and duplication** (backup lines, alternative routes, ring schemes where feasible);
- 2. Sectionalization and control of the grid** (the ability to quickly disconnect damaged sections while maintaining supply to critical nodes);
- 3. Standardized fast-deployable solutions** (mobile substations, transformers and other equipment items in stock within reach, plug-and-play solutions, ability for replacement by spare-stock items) – a logic that accelerates restoration time from weeks to days.

Play 4:

Consider Cascading Dependencies in Urban Energy Systems as a Distinct Risk

Ukraine's wartime experience — and Kyiv's winter of 2025-2026 in particular — has revealed a pattern that existing resilience frameworks do not fully capture. Under sustained attack, urban energy systems do not simply lose generation capacity. They shift from a mode of reliability optimization to a mode of systemic degradation, where the defining dynamic is not the scale of the initial strike, but the chain of consequences it triggers across interdependent infrastructure systems.

The Kyiv case, as well as similar experience of some other Ukrainian urban areas, illustrates this logic clearly. According to DiXi Group's estimates, the city's electricity deficit in January-February 2026 reached 35-45% of available winter generation capacity (DiXi Group's assessments) — a consequence of strikes on both local generation assets and the substations of the transmission backbone («Kyiv Ring») supplying the capital. However, electricity deficit spilled over to infrastructure systems that depend on stable power supply.

Water supply provides a direct example. Following the [January 20, 2026, attack](#), the left bank of Kyiv lost supply across all three districts simultaneously, while the right bank experienced

pressure loss only. This asymmetry reflected differences in structural exposure, not in the scale of the strike itself. More critically, as attacks continued through February, [available evidence](#) suggests that disruptions in a number of buildings had crossed a critical threshold: in-house piping that had not been drained in time has frozen and started bursting — physical damage that could not be reversed by restoring power supply alone, and that required complete repairs or replacement only feasible after temperatures rose above zero. While the full scale of such cases was not officially confirmed, the pattern itself signals a category of consequence that contingency frameworks must explicitly account for.

Public transportation faced similar constraints. Subway operations — accounting for 71% of all urban electric transport [according to passenger traffic data](#) in 2025 — could not be curtailed due to their critical role in mobility; surface electric routes absorbed the energy cuts instead, with diesel buses deployed as a demand-side energy conservation measure. The city's 45,000 personal electric vehicles faced a dual problem: [only 1 in 4-5 public fast charging stations remained operational during emergency outages, while subzero temperatures of -15°C reduced battery range by 20-40%](#).

Food retail continuity depended on small diesel generators — a backup that proved unreliable in the conditions under which it was needed most. At 0°C and below, standby generators [experience significant capacity degradation](#) — **effective output can drop to 70% of rated capacity at -10°C, with batteries losing up to 30-50%** of charge capacity at freezing temperatures; diesel fuel gels in extreme cold; and units designed for 8-12 hours of continuous operation were required to run around the clock through the winter.

Four structural lessons follow from this pattern. First, seasonal stress is a force multiplier, not a background condition. Winter peak demand does not simply increase load — it compresses the time 'window' between a manageable deficit and irreversible consequences across multiple infrastructure systems simultaneously. Contingency planning that does not explicitly model seasonal amplification will systematically underestimate urban risk.

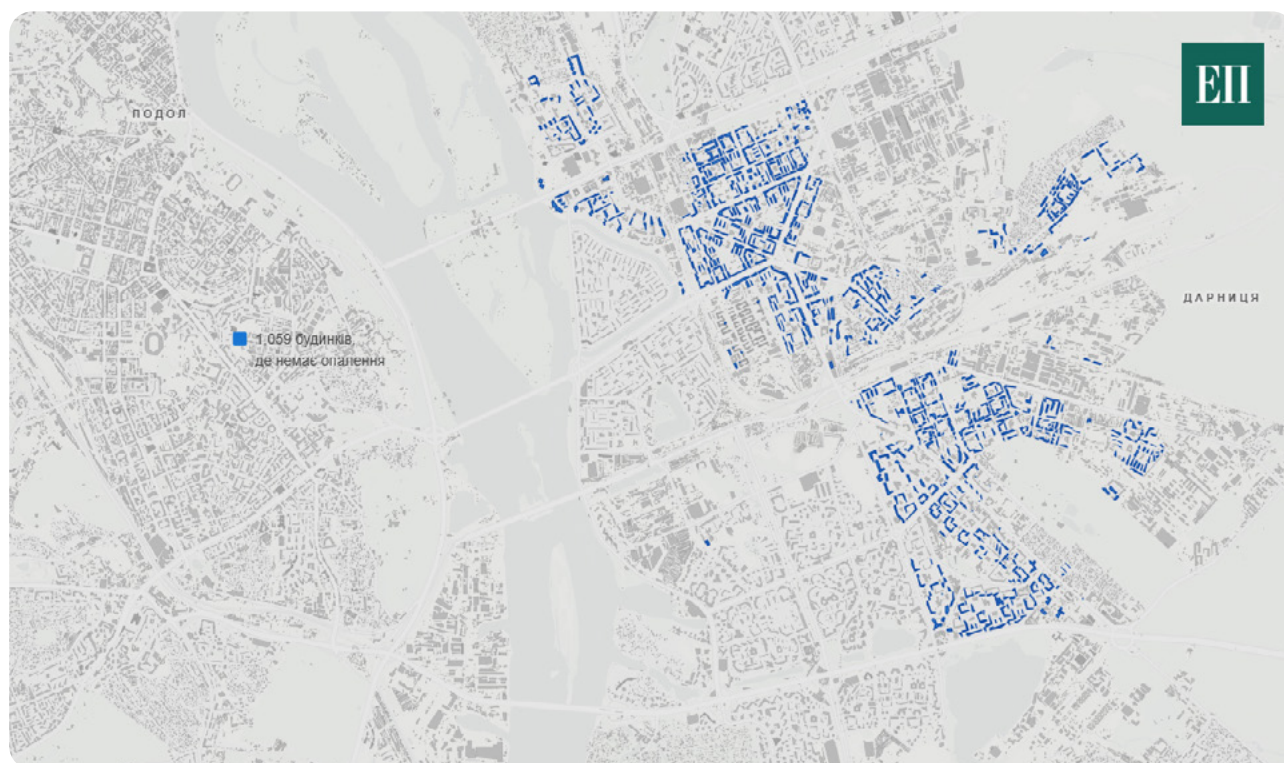
Second, technical limits change the character of recovery. Below a certain threshold, e.g. when pipes get destroyed by freezing, generators fail under sustained load, or cumulative infrastructure fatigue accumulates — restoring power supply no longer reverses the damage already done. Identifying and protecting these limits in advance is a qualitatively different planning task from general resilience investment. A decisive factor are human resource: availability and skills of specialists able to suspend operations within large-scale urban systems or conduct preventive measures.

Third, distributed backup power mitigates but cannot offset structural loss. Kyiv's district heating system [had deployed](#) 136 backup generators, 15 cogeneration units, and 69 mobile boiler units before the winter — and this allowed the system to remain broadly functional. However, it could not compensate for direct strikes on the three centralised CHPs that together supply 47% of the city's installed heat capacity (DiXi Group estimates, based on the [2030 Kyiv District Heating Scheme](#) presentation). Backup systems are buffers against temporary outages, not substitutes for the protection of critical generation nodes.

Fourth, urban infrastructure requires cross-system resilience frameworks, not sector-by-sector planning. Electricity, district heating, water supply/sewerage, public transportation, and food retail are not parallel and independent systems — they are interconnected, with disruptions propagating and accumulating over time. Planning frameworks that optimize

resilience within individual sectors, without mapping cross-sector dependencies and propagation chains, will miss the dominant failure mode under sustained attack conditions.

Buildings without District Heating due to Damage to the Darnytsia CHP (Kyiv)



Source: [Economichna Pravda](#)

Practical implications for public policy and investment planning:

- **Map cross-sector dependency chains as a standard planning instrument.** Urban resilience planning should explicitly model how electricity supply disruption propagates into district heating, water, transport, and essential services — identifying the sequence, timing, and reversibility of cascading effects. This dependency mapping should be a standard input to city-level emergency preparedness frameworks, not only a post-incident reconstruction exercise.
- **Define and protect urban limits of irreversible changes.** For each dependent infrastructure system, identify the point at which disruption transitions from a restorable outage to physical degradation — frozen and burst pipes, generator failures under sustained load, cumulative fatigue in aging networks etc. Protection and contingency measures should be calibrated to prevent crossing these thresholds, keep integrity of engineering systems or avoid damage to extent possible.
- **Design backup systems for the most extreme conditions under which they will actually be used.** Distributed backup — generators, mobile boilers, UPS — must be specified and tested for winter peak conditions, not average annual ones. Capacity ratings at weather extremes, fuel supply logistics in demand spikes, and continuous-operation endurance should be explicit procurement and deployment criteria.

- **Introduce winter-specific contingency planning as a distinct operational regime.** Seasonal stress amplifies vulnerability across all dependent systems simultaneously. Contingency plans that do not model winter peak demand, reduced backup output, and compressed recovery ‘windows’ will systematically underestimate urban risk during the period of highest exposure.
- **Audit infrastructure investments against wartime dependency risks.** Investments made under decarbonisation goals — EV charging networks, electrified transport, heat pumps — create new dependencies on uninterrupted electricity supply. As these assets scale, their behaviour under conditions of structural electricity scarcity should be modelled and managed as part of energy security planning.
- **Treat centralised urban heat sources as dual-priority assets.** CHPs and large boiler houses simultaneously function as electricity flexibility resources and as the primary source of district heating supply. Their protection, backup configurations, and recovery prioritisation should reflect this role — and be coordinated across operators and municipal authorities rather than managed through separate sectoral frameworks.

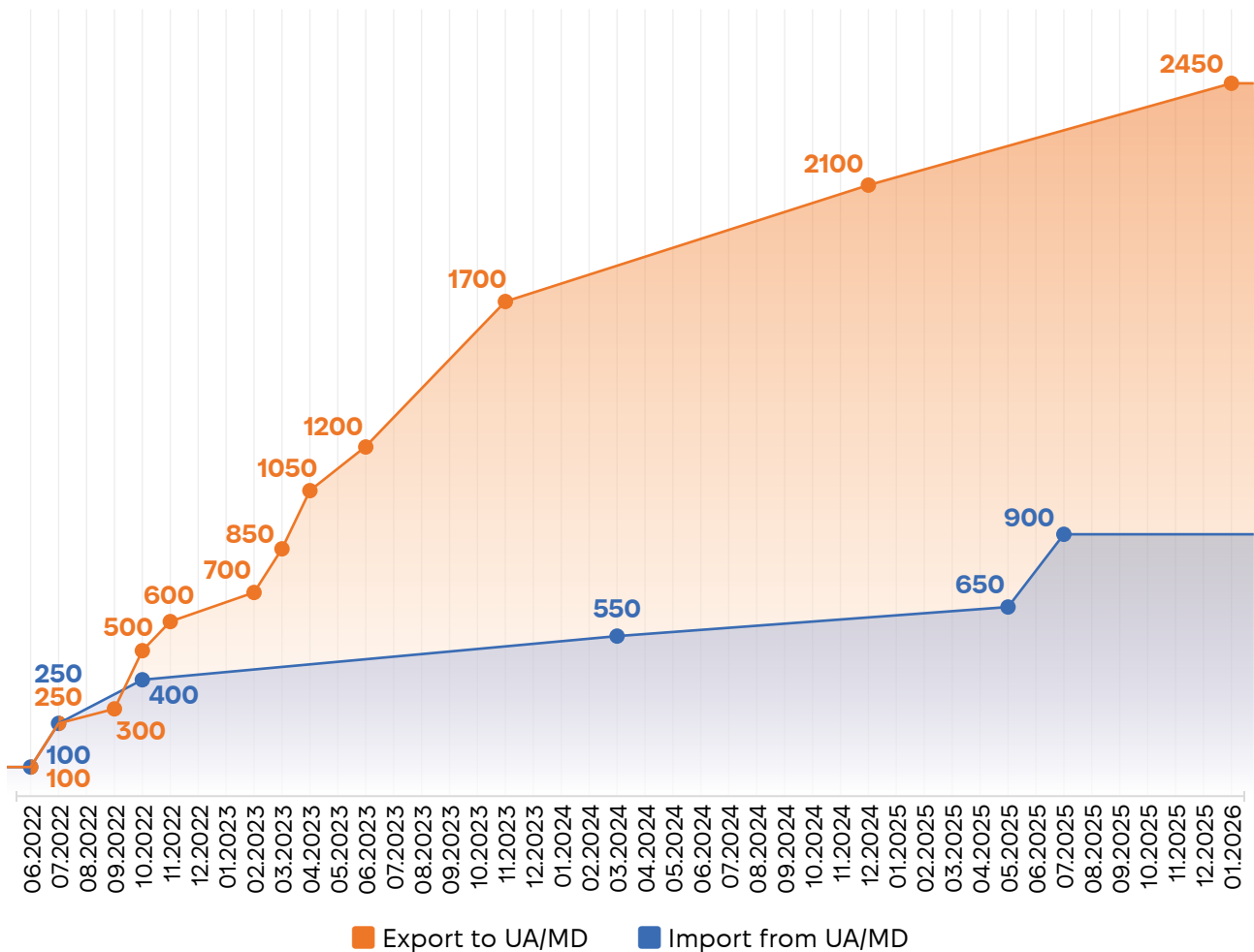
Play 5:

Ensure Interconnectivity as a Strategic Resilience Factor, but Account for Constraints

The synchronisation of the power systems of Ukraine and Moldova with the Continental Europe Synchronous Areas of the ENTSO-E in March 2022 was a strategic step that expanded options for emergency support, commercial exchanges, and deeper integration with the European electricity market. At the same time, wartime operations showed that the resilience factor of synchronisation depends not only on formal access to cross-border interconnectors, but also on a set of technical and operational constraints that must be explicitly incorporated into planning.

Since synchronisation, the agreed commercial import/export capacity from Continental Europe has been increased step-by-step as technical assessments and operational experience allowed. The timeline below illustrates how the permitted limits grew from an initial 100 MW in mid-2022 to much higher levels by 2024-2026. Importantly, these figures reflect a safety-constrained commercial exchange capacity agreed by European TSOs (not the nominal physical transfer capacity of interconnectors) - and therefore remain subject to periodic reassessments.

Evolution of the agreed capacity limits between Continental Europe and Ukraine/Moldova block, MW



Source: ENTSO-E and NEC Ukrenergo statements

Constraint 1:

Cross-border transfer capacity limits (NTC/ATC)

After synchronisation (March 2022), Ukraine gained more opportunities for commercial trading and emergency support, which increased system resilience. However, the volume of allowed cross-border flows is not a political decision – it is determined by stability and operational security calculations. ENTSO-E explicitly describes its approach as maximising flows “while ensuring power system stability and operational security” while [communicating increase in the export capacity limit to Ukraine/Moldova block](#) back in late 2024 with the possibility of further reassessments. Yet even if neighboring systems have sufficient generation capacities available, the real deficit is shaped by whether the recipient system can physically and safely accept and transmit additional megawatts through cross-border interconnections.

Constraint 2:

Limited number entry/exit points and their availability

Commercial imports are performed through specific interconnections (e.g. Ukraine with Slovakia/Hungary/Romania/Poland). When part of the related equipment in the transmission

system is under repair, damaged, or operating with constraints, the overall limit declines even if price signals and demand would otherwise incentivise imports. [This consideration aligns with the Energy Community Secretariat point](#) that, after the 2024 strikes, deficits intensified and “network bottlenecks” emerged, leading to outages/restrictions across the country.

Constraint 3:

Internal transfer corridor limits

Integration with ENTSO-E strengthened the ‘western gates’, but without relieving internal transfer constraints Ukraine faced asymmetry. Even if more power can be imported at the western border, a classic “bottleneck” arises further in the system: whether these volumes can be delivered to areas with higher deficit. This has already been [officially articulated as a priority](#) – implementing projects to improve electricity transmission from western to eastern part of the country to enable effective use of generated and imported electricity.

Constraint 4:

System services and control under stressed operation

Synchronisation provided Ukraine/Moldova with additional stability and opportunities for balancing and emergency supply. But the more the system operates ‘on the edge’ (damage management, switching, flexibility deficit), the stricter the transmission limits become – as cross-border flows affect frequency stability and voltage/reactive power management regimes. A deficit of flexibility amplifies network constraints – and vice versa.

Constraint 5:

Variable NTC limits and the procedural reality of integration

Import capacity for the Ukraine/Moldova block is defined monthly within the Eastern Europe Capacity Calculation Region (EE CCR). [In January 2026 it increased to 2,450 MW](#), up from the previous value of 2,150 MW. Therefore, integration is not a static fact but a continuous engineering and operational optimisation of NTC limits in line with risks and the condition of the systems operation within the respective CCR.

Naturally, there are also risks for the Continental Europe Synchronous Area when Ukraine/Moldova operate synchronously with it (shared frequency), as well as risks on cross-border interconnections (flows/voltage/protection and control). By way of example, the main risks include:

- **System stability risk (dynamic stability and frequency).** In a synchronous area, disturbances (sudden loss of lines/generation, unstable regimes) can potentially ‘echo’ into neighbouring systems – hence the ENTSO-E repeatedly emphasises that any increase in flows is made only under conditions of [stability and operational security](#).
- **N-1 compliance and congestion risk (steady-state security).** For European TSOs it is critical that even with the loss of a single largest element (N-1 criterion) the system remains secure. This principle underpins how ENTSO-E calculates available NTC limits with Ukraine/Moldova.
- **Risk of ‘unpredictable physical flows’ (deviation from scheduled flows).** Even if a flow is commercially scheduled, real physical flows may deviate due to emergency

configurations, network constraints, etc. Therefore, calculations include a reliability margin / TRM ([referenced at 250 MW as an uncertainty buffer](#)).

- **Risk of emergency incidents with resulting disconnection (system separation).** [ENTSO-E officially reported](#) that on January 31, 2026, an incident occurred that resulted in significant outages and the separation of Ukraine and Moldova from Continental Europe.

Synchronisation also creates shared operational responsibilities and risk considerations for the broader Continental Europe Synchronous Area, including system stability, N-1 security, congestion management, and uncertainty of physical flows under stressed conditions. This is precisely why expansion in cross-border net transfer capacity is necessarily linked to stability and operational security assessments. The practical lesson is not to consider cross-systemic integration as an unlimited support tool for resilience, but to treat it as a critical strategic asset whose value depends on a set of own system stability.

Play 6:

Standardise Equipment and Repair Approaches to Accelerate Recovery

Ukraine's experience in the energy sector recovery has demonstrated that the speed of restoring electricity supply depends not only on available funding or the number of deployable repair crews, but on how standardised the solutions and equipment requirements are – and whether this hardware can be quickly delivered, installed, and commissioned into operation.

In wartime conditions, such a strategy is not always possible, given that sometimes the choice is limited to available equipment (especially, donated hardware which was previously in use). However, the logic of standards is a shift from the individual approach (“each facility is unique”) to sets of typical solutions deployed as ready-made modules, minimising the time required for design, procurement, approvals, and installation/assembly.

Several considerations speak in favour of standardisation:

- 1. Narrow repair ‘windows’ and personnel security risks.** When assets are repeatedly hit or access to sites is unstable (e.g. areas close to the frontline), solutions that require minimal time for installation and commissioning are most valuable.
- 2. Shortage of unique equipment and long manufacturing lead times.** At the transmission level, autotransformers, current and voltage transformers, and switching equipment at typical voltage levels are critical; their production can take months, and ‘off-the-shelf’ solutions are scarce.
- 3. Complex character of international assistance.** Humanitarian aid supplies often arrive in batches with differing composition; so standardised specifications and typical solutions facilitate contracting/allocation, resolve compatibility issues, and accelerate commissioning (e.g. [transfer of transformer substations and other equipment to communities and DSOs](#)).

4. Operational logic of restoration. In late 2025 and early 2026, the speed of emergency repair works and the availability of equipment were key factors in determining whether strikes translated into prolonged blackouts.

First and foremost, standardisation is needed for equipment ‘packages’: e.g., for restoring substations (transformers/autotransformers, current/voltage transformers, protection relays and control components); for restoring overhead lines (conductors/ground wires, insulation, fittings, poles/towers, grounding, switching); and for critical urban distribution nodes (cabinets/switchgear cells, cable accessories, switching elements). In this context, [the approach reflected in the World Bank documents](#) is illustrative: given that large substation equipment (in particular 750/330/220/110 kV autotransformers) were among the most urgent needs for Ukraine’s energy system recovery, it was also noted that such equipment is difficult to source and move quickly due to differences in parameters and limited availability. This is why the unification of specifications and ‘lists of standard items’ (linked to typical voltage levels and grid nodes) reduces the time between damage and delivery.

Equally important is the standardisation of solutions like mobile substations and plug-and-play hardware. Ready-made engineering solutions become essential, reducing recovery time from weeks to days – pre-configured mobile substations and transformers; plug-and-play solutions with standardised connection interfaces and typical protection/SCADA schemes; and typical ‘temporary schemes’ for supplying critical loads.

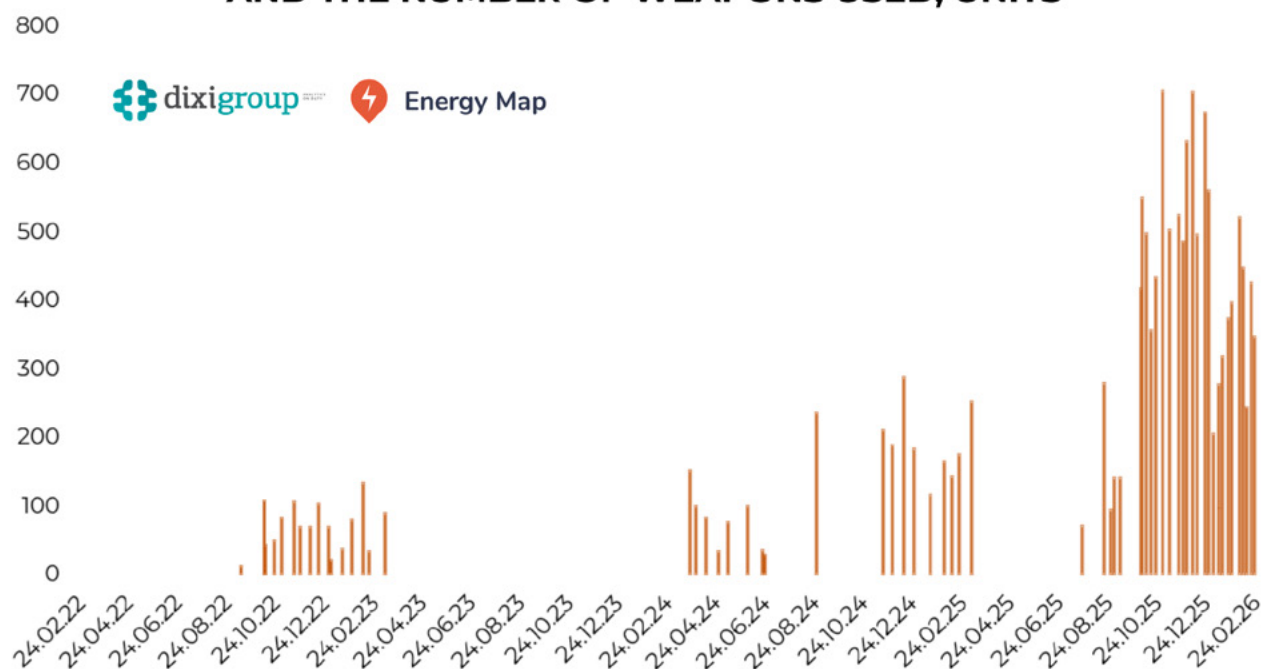
Standardisation of inventories and ability for replacement of components plays one of the key roles. Repair logistics must not break down because of a single ‘sub-standard’ element; therefore, compatible and standardised nomenclature of critical spare parts and prepared warehouse hubs (with transparent inventory tracking) for typical recovery scenarios are required.

Play 7:

Integrate Air Defence, Physical (Engineering) and Cyber Protection into Energy Security Planning

The aggressor’s military actions – and, above all, air attacks – have demonstrated a shift in the very understanding of energy security: under conditions of systematic aerial strikes, it ceases to be only a matter of capacity-demand balance or the speed of repairs. Also, massive attacks on Ukraine’s energy system facilities were frequently accompanied or preceded by significant cyberattacks on operators and market players. In such circumstances, a comprehensive notion of energy security includes the power system’s ability to survive under attack. This implies integrating two complementary components: active protection (air defence / electronic warfare / cyber protection) and passive (engineering) protection of facilities and personnel. This multi-domain approach to protection is now articulated as a policy priority: e.g., physical protection is deployed in parallel as an instrument to reduce losses from repeated attacks and new facilities are designed in a way to integrate this component to a maximum extent possible.

WAVES OF MASSIVE ATTACKS ON ENERGY INFRASTRUCTURE AND THE NUMBER OF WEAPONS USED, UNITS



Source: [DiXi Group](#)

Air defence may not be considered a function of energy companies – it is the responsibility of the defence sector. However, the recent [decision](#) of Ukraine’s government to enable development of operators-led defence capabilities might be a game-changer. However, this step should not be treated as creation of ‘private armies’, as air defence units created would operate under full command and control of military authorities. Such facility-based units will complement the multi-layer system of air defence critical for the power system. Timely detection and interception of targets reduces the frequency and scale of damage, decreases the need for emergency outages, and stabilises system operation during peak periods. In this sense, requests to allies for air defence and counter-UAV/missile capabilities are framed not merely as a ‘general defence need’, but as a condition for maintaining the functionality of critical services (electricity/heat/water/communications/healthcare etc.).

Even with a high density of air defence cover, including SAM systems of different range, mobile fire groups with MANPADs, anti-aircraft guns, and interceptor drones, air force units and as well as jamming, spoofing and other types of electronic warfare, it is impossible to “close the sky” completely – the adversary adapts tactics and combines different means of attack. Therefore, passive protection is viewed as the ‘last line of defence’, reducing the probability of critical damage to key equipment, shortening recovery time, and lowering the risk of cascading accidents. This logic is directly embedded in [decisions on the security of critical infrastructure facilities](#): priorities include counter-drone measures, alert and warning systems, personnel shelters, backup control points, and organisational security components.

In practical terms, passive (engineering) protection in the electricity sector performs three functions:

- 1. Preserving expensive/scarcely equipment** (primarily at key substations and generation facilities) to prevent the lack of elements with long replacement lead times.
- 2. Reducing the repeated losses:** under cyclical attacks, it is critical that a facility does not degrade faster than it can be restored.
- 3. Improving ability for repair and personnel safety:** enabling work within short repair “windows” and reducing risks for repair crews.

Ukraine’s model for protecting energy facilities has evolved from post-strike repairs towards an institutionalized yet constantly evolving architecture. At the level of national policy, the need to reinforce security of critical infrastructure facilities is articulated, including counter-drone instruments, shelters, backup control points, and other resilience elements. A dedicated coordination mechanism for physical protection has also been established. In particular, [a coordination format was created](#) that focuses on frontline regions and brings together the energy sector specialists, infrastructure authorities, and regional administrations.

Designing protection measures under wartime conditions cannot follow a ‘classic construction’ approach with long cycles, because facilities are attacked repeatedly. Therefore, the key managerial conclusion is that typical (standardised) engineering solutions are needed – solutions that can be rapidly adapted and scaled up. [Official communications report](#) the development and approval of a package of standard engineering solutions jointly with military engineers and relevant defence structures, with these solutions intended for use by all custodians of energy infrastructure. In parallel, [methodological/technical materials](#) are being published to guide the selection of engineering protection elements, reflecting a transition to a scalable approach rather than isolated, non-standardised solutions.

Recovery efforts have shown that protection must be embedded “by default” in modernisation and repair programmes. Therefore, despite higher capital costs, the “protection-by-design” approach should become a standard of investment planning: protecting key nodes (generation/transmission/critical urban hubs) should be planned and financed in the same way as other elements of the systems like transformers, protection and automation systems (relay protection).

A separate balance that will need to be maintained going forward is that transparency and accountability (especially for donor financing) must coexist with limits on the level of information disclosure that could create security risks for facilities. This does not remove the need for audits and performance control – but it changes the format and the level of public data disclosures.

Example of Level 2 engineering protection of an energy facility



Source: [Ministry for Development of Communities and Territories of Ukraine](#)

The basic logic of the national critical infrastructure facilities (CIF) protection system is as follows: the facility-level management and security are ensured by the operator (company/asset holder), while the government sets the rules, coordinates, and reinforces protection where massive investments and coercive/military instruments are required. This is explicitly stated that the facility-level component of the CIF protection system is ensured by the operator, while the regional/local levels involve responsible public authorities, including military administrations.

In practice, the responsibility of a CIF operator includes:

- organising protection measures at the facility and planning security and actions in crisis modes;
- protecting personnel (shelter/evacuation procedures/access control) and creating reserves of equipment and materials for repairs;
- readiness to operate under repeated attacks (backup power supply, protected documentation reserves, archiving critical data, etc.) – as the “on-site conditions” required to be in place.

Separately, the [Law of Ukraine “On Critical Infrastructure”](#) establishes that a [security passport](#) is a key instrument for planning the protection of a CIF (based on categorisation and threats assessment carried out by sectoral authorities jointly with operators under a [defined methodology](#)).

The government role is decisive in two areas:

1. Prioritisation and coordination of CIF protection nationwide. The National Security and Defence Council (NSDC) Decision of October 17, 2023, [directly sets](#) state priorities (counter-drone measures, warning systems, personnel shelters, backup command posts, etc.) and assigns tasks to the government/sectoral authorities and military structures for organising physical and engineering protection.
2. Military dimension – air defence/defence/guarding as the competence of the security and defence sector. Air defence coverage, guarding, and defence of CIF involve units of the Armed Forces of Ukraine and the National Guard; the list of important state facilities (critical infrastructure) subject to air defence coverage is determined by the Cabinet of Ministers of Ukraine. The mentioned decision to delegate certain functions to the operator still includes full command and control of the military.

Additionally, under martial law, the military command together with local military administrations may establish/strengthen the guarding of CIF and introduce a special operating regime for them; the list of such facilities and the procedure are approved by the Cabinet of Ministers.

In practice, the decision on the level/priority of protection consists of two interconnected tracks: categorisation (criticality) of the facility, and government determination of facilities for guarding/defence/air defence. The NSDC decision establishes that the Cabinet of Ministers, together with the General Staff, monitors and updates the list of facilities requiring priority air defence coverage. Separately, the legal framework also indicates that the list of CIF with guarding to be carried out by state bodies/enterprises is approved by the Cabinet of Ministers, and that the National Guard provides guarding of CIF according to the list approved by the government.

The direct 'inputs' for categorisation and protection prioritisation are network criticality, key consumers, and key producers/sources.

Network element criticality (a nodal substation, an interregional corridor, an asset with a high system-wide effect) directly affects categorisation given the anticipated consequences of functional disruption and the scale of impact on vital services/functions.

Key consumers (water utilities, district heating, healthcare, communications, defence/critical manufacturing) matter as a criterion of societal impact: the law defines critical infrastructure through the provision of vital functions/services, and the NSDC decision separately emphasises the need to take consumer priorities into account when applying restrictions.

Key producers/sources (generation, dispatching control nodes, urban heat generation) influence decisions not merely through their capacity, but rather system role – the ability to sustain critical services and prevent cascading accidents.

Regional/municipal military administrations are the key territorial coordinators – ensuring interaction of military with operators, the State Emergency Service, and responsible ministries regarding engineering protection, reserves, shelters, fencing, facility readiness, and response regimes. The police and other law enforcement authorities, in turn, typically are responsible for law and order, regime measures, responding to offences/sabotage threats, supporting access-control regimes, and ensuring security around facilities within the state-defined regimes.

Play 8:

Build Logistics Resilience, Reserves, and Clear Prioritisation for Supplying Primary Energy Sources

The motor fuels segment became one of the first targets at the start of the full-scale invasion: attacks were directed at refineries, oil depots, and logistics hubs, which have quickly “reset” the pre-war model where a significant part of the supply chain relied on large, centralised storage and processing facilities. Attacks on the gas sector in later stages of the war also indicated several vulnerabilities for energy balance, given its role in district heating, industrial processes but also electricity generation. For that reason, the oil&gas sector became part of the same resilience logic as the power sector: the key was not merely to have the resource, but to have manageable supply chains, reserves, and clear prioritisation rules.

Anti-crisis measures taken by the government of Ukraine to facilitate the shift to imported motor fuels (petroleum and diesel):

- Reducing VAT on fuel from 20% to 7% and abolishing the excise duty to lower prices and incentivise imports. This measure, applicable from March 2022 until July 1, 2023, [was explicitly communicated as an instrument to stabilise the market](#);
- Price deregulation under shortage conditions: in May 2022, the government [abandoned retail price regulation for petroleum and diesel](#) so that operators could “saturate” the market faster;
- Simplifying import operations: the government approved lists of goods for critical imports to prioritise trucks border crossing and ensure operational manageability of supplies.

Physical decentralisation of storage (moving away from a few large depots) in wartime conditions naturally became a combination of regulatory framework and market players behaviour.

[At the policy level](#), Ukraine is moving towards a system of minimum stocks of crude oil and petroleum products (following the EU regulations), where the formation of reserves and the rules for their application in a crisis are set by law/government, while the storage infrastructure itself may be distributed across multiple entities and locations. E.g., for the period of martial law and 6 months after its termination/suspension, up to 50% of minimum stocks can be created in the neighboring and adjacent EU member states (subject to storage facilities availability and connection to reporting system).

In practice, while the minimum stocks are yet to be fully formed, fuel supply is subject to prioritisation.

State/military demand as first priority (defence, emergency services, critical infrastructure) is covered via centralised procurement and coordination with market players. While commercial prioritisation is performed through contractual and logistical arrangements (advance payments, long-term contracts, dedicated supply channels).

For natural gas, prioritisation is significantly more formalised due to the PSO (public service obligations) regime and the concept of protected consumers. The state maintained and expanded the [PSO](#) regime applicable for households and other consumers like district

heating companies (gas volumes used for the needs of households, enjoying fixed pricing and supply conditions, which in practice means prioritising household needs). The legal framework of the natural gas market also defines consumer categories and, under the logic of security of supply, identifies those for whom uninterrupted supply is socially critical: households, other facilities as an element of basic life-support in urban areas, and district heating enterprises servicing these two categories).

For non-military industries, the practical implication is that during shortages, such industrial consumers more often have to operate in an adaptation mode reacting to price signals and supply interruptions (contracts hedging, voluntary demand reduction, fuel switching etc.). At the same time, certain enterprises may receive higher priority if they are formally classified as critical (due to their role in security, vital supply chains, or support of critical services). Such entities, as per [the Security of Natural Gas Supply Rules](#), include:

- entities producing foods intended for daily consumption, foods of animal origin, including those related to the processing of perishable products;
- entities ensuring waste processing;
- healthcare institutions, emergency and rescue services, law enforcement agencies, bodies and institutions for the execution of sentences, water supply and sewage facilities, crematoriums;
- other public authorities, local self-government authorities.

Play 9:

Strengthen Crisis Communications and Grassroot Preparedness

Communications and public preparedness have become an element of operational resilience: they influence demand behaviour, help reduce peak loads, and mitigate the humanitarian consequences of disruptions. During periods of generation deficit or grid damage, effective communication serves to manage demand behaviour (peak loads reduction, managing 'postponed demand'), reduce panic reactions, and maintain trust in dispatching decisions and system operators.

In parallel, preparedness practices adopted by households, commercial sector and communities have reduced the humanitarian impact of outages (water/heat/communications/healthcare etc.), lowered the burden on local services, and increased cities' ability to endure prolonged periods of restrictions.

A critical lesson is that [transparent explanations of the causes and types of restrictions](#) directly affect perceptions and willingness to accommodate to constraints. At the level of public institutions and regulatory/supervisory communications, it is emphasised that scheduled hourly outage schedules and emergency outage schedules follow different application logics and serve as instruments to stabilise system operation under deficit conditions or during emergency events.

It has become important to consolidate a model in which the TSO (Ukrenergo) communicates the overall state of the power system, the need for restrictions, and general recommendations on consumption; the DSOs on regional level provide practical, 'address-based' information (outage lines/hours) with near-to-real-time updates; and local authorities and civil

protection services focus on safety, life-support services, and support for vulnerable groups. This approach of right channel for the right message is explicitly reflected in the TSO communicating that the time and scope of outages should be checked on the official resources of a relevant DSO.

In many crisis episodes, the most destructive factor for trust was not the very fact of outages, but the gap between expectations and reality – when forecast/scheduled hourly schedules were not followed due to emergency events, repeated attacks, or abrupt changes in the system balance. Therefore, one of the key lessons has been the [systematic explanation of the difference between planned/stabilisation restrictions and emergency outages](#), as well as the logic of transitioning between them. This issue has been officially clarified as part of crisis communication.

A practical conclusion for communication policy is that every message about restrictions should include:

- the **reason**,
- the **relevant time horizon**,
- an **address-based verification source**,
- **expectations regarding possible deviations** (especially when the risk of switching to emergency outages is high).

Preparedness of households, businesses and communities has become an element of the grassroots layer of energy resilience: it does not replace the restoration of generation/grids, but it reduces cascading impacts on water supply, heating, communications, healthcare, and other elements of urban safety.

[The State Emergency Service systematically publishes recommendations on life-support and safety during electricity outages](#) (water/food stocks, lighting, safety rules, etc.), similar communications are frequently made by the National Police. At the level of urban infrastructure, similar materials (household preparation, water and non-perishable food reserves, planning family needs) are formalised as [official public guidance notes](#). Business practices include adapting to emergency mode of operations with own sources of generation or back-up power supply. In some cases, they are facilitated by regulations – e.g., to provide uninterrupted Internet and telecommunication services, requirements were introduced to operators (with gradually increase of expected duration for offgrid operation for all basic stations) along with free ‘national roaming’ scheme (ability to switch operators if connection is lost). However, in most examples, these are own or collective initiatives – e.g., POWER BANKING network covering over 50% bank offices and capable of withstanding multi-day outages.

The lesson for energy and related policies is twofold:

- basic ‘energy literacy’ (understanding types of restrictions, peak hours, and the logic of demand response as a system tool) helps reduce peak load, after-outage spikes, and the frequency of shifts into stricter regimes;
- local actors (households, businesses and municipalities) preparedness lowers social tension and the need for emergency interventions (especially during the first 24-72 hours of prolonged outages).

A separate organisational solution has been the network of resilience centres (**Points of Invincibility**) as a response to the risks of long outages and the degradation of basic services. Such centres were created by governmental and municipal institutions, in some cases even businesses, and operate both as stationary and deployable (i.e. ready to be opened very fast). From early on, such centres have to operate under [the set standard](#), which includes 24/7 regime, xPON/Starlink Internet connection, autonomous power supply for device charging, heating devices, means for preparing hot drinks and food, drinking water and other typical essential services. For energy resilience, this is important not only as humanitarian support to the population, but also as an instrument for stabilising the urban energy consumption, thereby reducing secondary losses from outages.

At the same time, wartime communications must be designed as part of resilience against disinformation. In the case of Ukraine, the Russian state and affiliated information actors, including media, proxy channels, and coordinated online influence networks, exploited outages and infrastructure damage to spread panic, erode trust in operators and public authorities, and trigger destabilising consumer behaviour (e.g., panic buying of fuel and generators, surges in simultaneous electricity use after restoration announcements). In this sense, communication failures can translate into operational stress for the energy system.

This makes crisis communication a systemic management function rather than only a public information task. In practice, communication systems should include monitoring of information space, message synchronisation across institutions (TSO, DSOs, local authorities, emergency services, and government entities), agreed templates for outage and restoration messages, and proactive public guidance that counters false narratives before they scale. Trusted local relay channels and targeted messaging for vulnerable groups are also essential to reduce humanitarian risks and improve compliance during prolonged disruptions.

Play 10:

Enable Industrial Adaptation through Backup Supply and Energy Management

Ukraine has historically been one of Europe's most energy-intensive economies, a structure supported for decades by relatively low-cost energy inputs, a nuclear-anchored baseload that kept electricity prices low, and an overreserves Soviet-era transmission system that enabled abundant domestic supply and exports.

This legacy matters for today's crisis response: heavy industry has been a structural driver of demand, and the war-time decline in energy demand is explicitly linked to reduced industrial activity alongside migration/displacement.

For energy-intensive industries, electricity supply disruptions translate into the risk of disrupted technological cycles, reduced product quality, equipment damage, and prolonged downtime due to the complexity of restarting processes. Therefore, the key business response has been a shift from the logic of "compensating outages" to the logic of controlling the consumption regime: enterprises began to treat electricity as a resource that must be dispatched within the industrial site in the same way the system operator dispatches the power system at the national level.

This adaptation may go far beyond back-up diesel generators and is based on a combination of organisational and engineering solutions. First, some companies have adjusted production schedules to available capacity: moved energy-intensive operations to night hours, started lines sequentially rather than in parallel, and introduced internal limits and load prioritisation. Second, short-horizon technological ‘buffers’ were deployed: UPS for critical automation/instrumentation and IT systems, as well as battery storage to smooth peaks, ride through voltage/frequency dips, and ensure the safe shutdown of specific units. Third, a separate focus has been placed on power quality: reactive power compensation, harmonic filtering, voltage stabilisation, and upgrades of automatic transfer switching/sectionalising schemes – reducing equipment failures under unstable regimes and lowering losses when supply is restored. In parallel, where feasible, companies were moving toward non-diesel sources for backup and baseline supply of critical needs: gas engine / cogeneration units, on-site PV plus battery storage, site-level microgrid configurations, as well as energy efficiency measures and optimisation of operational regimes (variable-speed drives, optimisation of pumping and compressor systems, and energy recovery).

From a system perspective, this transformation has a dual effect. For businesses, it reduces the risk of catastrophic shutdowns and converts supply shortages into a controlled operating mode with more predictable outcomes. For the power system, it creates an additional resilience resource on the demand side: when industrial consumers reduce peaks, spread loads over time, and can temporarily curtail secondary processes, the depth of restrictions and the frequency of transitions to emergency scenarios decrease. As a result, industry becomes an active participant in balancing – through energy management and demand response.

Play 11:

Use Regulatory Policy to Accelerate Reconstruction and Restore Market Stability

The full-scale war has turned energy sector regulation into an instrument of operational resilience: security has appeared not only preventing supply disruptions, but also the ability to rapidly repair, reconnect, and restart damaged assets. Accordingly, regulatory decisions in Ukraine can be viewed along two interconnected avenues: (1) accelerating the construction/reconstruction of energy facilities through procedural simplifications; and (2) stabilising market functioning and ensuring the system’s financial resilience under strikes, shortages, and liquidity risks.

1) ACCELERATING RECONSTRUCTION: DEALING WITH REGULATORY BOTTLENECKS AND WARTIME FAST-TRACKING

Practice has shown that recovery speed depends not only on resources, but on whether the government and regulators remove barriers at key stages — permits/authorisations to perform works, design and expert review, land use, grid connection/reconnection, procurement and contracting, and payment and acceptance of works. A series of simplifications were introduced that enabled faster works under short repair ‘windows’, equipment shortages, and the need to rapidly restore grid connectivity. To name a few most important ones:

- **A declarative principle for certain types of economic activity.** The [Cabinet of Ministers Resolution No.314](#) (2022), with further amendments, expanded the ability to

operate under a declarative principle for a range of procedures during martial law (as a general deregulation mechanism);

- **A special wartime procedure for deploying/commissioning generating units.** The [Cabinet of Ministers Resolution No. 1320](#) (2023), with further amendments, introduced a specific procedure for the construction and/or commissioning of certain types of generating units during the martial law as a response to the need to rapidly add capacity/reserves and decentralise energy supply;
- **Emergency procurement and fast contracting.** The [Cabinet of Ministers Resolution No. 1178](#) (2022), with further amendments, defined specific rules for public procurement during the martial law and for a period after its termination/cancellation, in order to shorten the cycle from need identification to delivery/works.

At the same time, acceleration could not be unconditional. Therefore, an important element in this approach consists of minimum safeguards for quality, safety, and integrity (technical/author supervision, acceptance procedures, evidence of volumes, control of pricing and payments), which should not disappear but rather be adapted to wartime conditions.

2) MARKET STABILISATION AND FINANCIAL RESILIENCE: RULES FOR THE “SPECIAL PERIOD”

Alongside deregulation of reconstruction, the government had to maintain the feasible operations of the electricity market: without settlements and liquidity, even available resources (repair crews, fuel, imports, assistance) do not translate into reliable supply. A key cornerstone was the introduction of [special regulatory regimes for market operation during martial law](#), including measures aimed at preserving the financial resilience of market participants.

Subsequently, regulatory policy evolved around balancing two objectives:

- preventing destructive price/financial shocks and unmanaged debt accumulation,
- maintaining investment and operational signals (so that imports/generation/repairs are not ‘switched off’ due to non-feasibility).

An example of this balance are price caps on the day-ahead and intraday markets, as well as on the balancing market. In particular, the National Energy and Utilities Regulatory Commission (NEURC) has set such price caps as temporary measure at the launch of the new market model in mid-2019, while during the war this instrument has become a permanent one with revisions/updates reflecting changes in system conditions, import opportunities, and risks of deficit.

3) INSTITUTIONAL MECHANISMS SUPPORTING RECOVERY

Ukraine’s war experience has shown that part of recovery inevitably relies on **non-market instruments** for rapid financing and supply, especially for scarce equipment. In this context, the dedicated Ukraine Energy Support Fund has been important, accumulating donor contributions for equipment procurement and rapid response to emerging needs.

This is an example of how a regulatory/institutional architecture can accelerate recovery when classical market mechanisms (investment programs or budgets) cannot keep up with the scale of damage and losses.

PART III:

THE AGENDA — FROM WARTIME ADAPTATION TO RESILIENCE BY DESIGN

The eleven principles documented in this Playbook were drawn from a type of crisis that has no direct parallel — and this distinction matters for how they should be interpreted and applied.

The reference points that have shaped energy resilience policy in recent years were crises of a fundamentally different character. The Texas winter storm of February 2021 was a bounded weather event: generation assets that had not been winterised failed simultaneously, the system collapsed within hours, and recovery began as soon as temperatures rose. The European gas crisis of 2021-2022 was driven by market dynamics — supply tightening, storage underinvestment, and demand spikes — that created price and supply stress but left physical infrastructure intact. California's repeated wildfire-driven outages have been managed through controlled load shedding, with recovery measured in days. Even the collapse of Puerto Rico's grid after Hurricane Maria — one of the most severe infrastructure failures in a modern economy in recent decades — was ultimately a restoration problem: the grid had to be rebuilt, but it was not being destroyed again while reconstruction was underway.

Ukraine's situation differs in a structural sense, not merely in scale. The threat is not a bounded event after which recovery can begin — it is a sustained campaign in which assets are struck repeatedly, repair 'windows' are constrained by ongoing attacks, and the adversary deliberately targets the bottlenecks that would otherwise enable recovery. Infrastructure that is restored becomes a target again. The system does not move from crisis to recovery; it operates permanently in a degraded mode, adapting to cumulative damage while under continued pressure. Existing resilience frameworks — built around the sequential logic of shock, response, and recovery — were not designed for this dynamic.

The principles in this Playbook represent operational knowledge extracted from four years of wartime energy sector management. They are grounded in real decisions made under real constraints, with observable outcomes.

At the same time, this Playbook is not a completed research product. Several findings rest on evidence that is partial or hard-to-verify-externally given the lack of publicly available data. The conditions under which Ukrainian operators worked — information security constraints, rapidly changing system configurations, the absence of normal data collection cycles — made systematic documentation often impossible in real time. Much of what is captured here reflects the judgement of practitioners.

The principles also interact with each other in complex ways. Grid resilience and flexible generation reinforce each other, but the optimal balance depends on system topology, attack patterns, and recovery logistics that vary across contexts. The effectiveness of standardisation depends on supply chain conditions that may not hold elsewhere. These are not arguments against acting on the principles identified here — under wartime conditions,

waiting for more complete evidence is not an option. They are arguments for treating this Playbook as the foundation for a sustained research agenda, not its conclusion.

As a foundation for further research, several questions emerging from Ukraine's experience warrant deeper investigation — both to strengthen the analytical basis of the principles identified here, and to support their application in other contexts.

Without granular data series, the dynamics of cumulative infrastructure degradation under repeated attack are poorly understood. Existing engineering and policy frameworks model individual failure events; they do not model the trajectory of a system that is repeatedly damaged and partially restored over months and years. Ukraine's documented experience is the primary empirical source available for developing this understanding.

The economics of wartime energy resilience have not been systematically examined. What is the cost-effectiveness of different protection strategies? How should standardisation investments be prioritised across a large and heterogeneous grid? What is the value of cross-border interconnection capacity under different attack scenarios? These questions are tractable, but require data and methodological frameworks that do not yet exist for the wartime context.

The transferability of Ukraine's experience to other contexts — European countries planning for energy security under geopolitical pressure, or economies facing similar infrastructure vulnerabilities — requires vigorous analytical work. Not all principles transfer directly. Grid architecture, institutional conditions, supply chain access, and threats environment differ in ways that affect which lessons apply and in what form.

Finally, the human capital dimension of energy resilience remains largely undocumented. Ukraine's energy sector maintained operational control through four years of sustained attack not only because of equipment and infrastructure decisions, but because of the people who operated and repaired the system under conditions of extraordinary difficulty. Understanding what that required — the skills, institutional knowledge, and organisational capacity that made it possible — and how it can be systematically maintained and preserved, is among the most important questions to be addressed.

This Playbook is offered as the foundation on which that research agenda can be developed: a structured account of what four years of sustained attacks on an energy system have produced, and what it demands of those who study and design the energy systems of the future.



www.dixigroup.org/en