Energy System Resilience

Lessons learned from Ukraine

International Energy Agency

INTERNATIONAL ENERGY AGENCY

The IEA examines the full spectrum of energy issues including oil, gas and coal supply and demand, renewable energy technologies, electricity markets, energy efficiency, access to energy, demand side management and much more. Through its work, the IEA advocates policies that will enhance the reliability, affordability and sustainability of energy in its 32 Member countries, 13 Association countries and beyond.

IEA Member countries:

Australia
Austria
Belgium
Canada
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Japan
Korea
Latvia
Lithuania
Luxembourg
Mexico
Netherlands
New Zealand
Norway
Poland
Portugal
Slovak Republic
Spain
Sweden
Switzerland
Republic of Türkiye
United Kingdom
United States

The European Commission also participates in the work of the IEA

IEA Association countries:

Argentina
Brazil
China
Egypt
India
Indonesia
Kenya
Morocco
Senegal
Singapore
South Africa
Thailand
Ukraine

Source: IEA.
International Energy Agency
Website: www.iea.org

Abstract

Ensuring energy security encompasses both long-term and short-term dimensions. The long-term dimension involves securing sufficient infrastructure investment and diverse supply sources. The short-term dimension – resilience – focuses on systems' ability to cope with events exceeding standard planning conditions. Since Russia's full-scale invasion in 2022, Ukraine has worked to protect its energy sector and to increase its ability to withstand and rapidly recover from Russia's attacks on its energy infrastructure. The report explores the lessons that Ukraine has been learning as it works to bolster system resilience and identifies measures that apply to a range of high-impact events – such as cyberattacks, physical attacks on infrastructure, extreme and severe weather, and unexpected infrastructure failures – and can in turn be adopted by policymakers and regulators around the world, taking into account national circumstances and following assessments of costs and risk.

The International Energy Agency (IEA) has worked closely with Ukraine, an Association country, on energy system resilience, publishing a 10-point plan ahead of the 2024-2025 winter, along with a 2025-2026 update and a roadmap for decentralising Ukraine's power system. This has provided Ukraine with critical assistance, while also offering invaluable real-world lessons that can inform resilience planning for IEA Member countries and beyond. Industry from Europe and other regions is already collaborating with the Ukrainian private sector and learning from practices forged under extreme conditions as they provide support. This report distils key lessons from Ukraine's experience that can inform energy system resilience efforts worldwide.

Executive summary

Ensuring the resilience of energy systems – or their capacity to prepare for disruptions, withstand shocks while maintaining operations, and rapidly restore service – plays a key role in managing many of today's emerging security risks, from weather disruptions to geopolitical tensions. Energy security encompasses both long-term adequacy through infrastructure investment and diverse supply sources, and short-term resilience for events beyond standard planning conditions. While countries face different threats – from extreme and severe weather to cyberattacks and infrastructure failures – a common challenge is to design adaptable systems that can respond rapidly, isolate affected components, and restore supply services swiftly when disruptions occur. While resilience investments require upfront funding, integrating resilience at the planning phase proves more cost-effective than retrofitting systems later or recovering from failures – and it delivers broader societal value by ensuring that critical services remain functional and daily life can continue should disruptions occur.

The resilience measures developed in Ukraine to bolster a system under extreme stress offer universal insights that transcend the specific context of armed conflict. The scale and systematic nature of Russian attacks on Ukraine's energy infrastructure – often compounded by severe winter conditions – represent a profound challenge. Since the onset of the full-scale invasion in 2022, Russia has exploited its detailed knowledge of Ukraine's energy system – inherited from the Soviet era – to strategically target critical nodes such as electrical substations. The resulting failure in these nodes disrupts connections to key generators and requires costly, time-intensive repairs. The measures Ukraine has taken to enhance energy system resilience under these extreme conditions – in many cases improvised, rather than the result of long-term planning – can provide broader lessons.

Since January 2026, Ukraine has faced a severe convergence of threats, creating a catastrophic humanitarian and energy crisis. Russian missile and drone strikes on electricity and gas infrastructure have intensified, and their impact has been compounded by one of the harshest winters in recent years. The power system has been hit especially hard. Ukrainian households have endured severe blackouts, with some areas – including the capital, Kyiv – losing access to power for 17 hours or more on a daily basis. As of mid-January, Ukraine's electricity demand reached 18 gigawatts (GW), while the power system's capacity stood at roughly only 11 GW – a 7 GW deficit that has forced rolling blackouts, threatened heating and water systems during severe sub-zero conditions, and endangered

essential services. In response to these extreme challenges, Ukraine has showed extraordinary determination to pursue a new architecture of energy resilience through decentralised electricity and heat generation, complemented by mobile generators and underground control systems.

10 lessons for energy system resilience

These 10 lessons, drawn from Ukraine's experience under extreme conditions, provide a toolkit of resilience measures that policy makers around the world can adapt and implement based on their own circumstances and cost-benefit analysis. For each lesson, the report provides a snapshot of how Ukraine has addressed these challenges alongside practical recommendations that policymakers and regulators can tailor to their national risk profiles and priorities.

1. **Put resilience at the centre of energy system planning.** Power systems designed for resilience return to normal operation far faster during extreme events and can avoid catastrophic societal impacts and costs. Integrating resilience at the planning phase – through holistic risk assessments involving operators, regulators and energy ministries – reduces overall costs compared with retrofitting and it should not slow planning processes if incorporated systematically.

2. **Implement physical hardening and defence measures**. Physical hardening protects infrastructure from both intentional threats and natural hazards, with many techniques providing cross-cutting protection regardless of the threat faced. Effective hardening combines infrastructure that is designed for protection with the ability to rapidly deploy equipment to shield priority assets during emergencies.

3. **Build comprehensive emergency response capabilities that cover multiple threat scenarios**. Effective emergency response requires trained teams, technical expertise, specialised equipment, and coordination mechanisms to respond rapidly under extreme conditions. Pre-established legal frameworks, decision protocols, and in-house technical capacity enable faster action than improvisation during crises.

4. **Ensure effective emergency communication mechanisms to reach citizens**. No single communication channel is perfectly reliable during extreme crises. Multi-layered systems where backup channels function independently – from battery-powered repeaters and radios to sirens and community networks – ensure critical information can reach populations when digital infrastructure fails.

5. **Leverage decentralisation and distributed resources as strategic security assets**. Distributed assets are inherently harder to target and easier to restore when damaged. They also allow for the maintenance of some essential services when interconnected systems are damaged and can help restart them in the event of disruptions. Enabling regulatory frameworks and intelligent grid platforms are essential to coordinate these resources as decentralisation grows.

6. **Maintain emergency oil stocks as a buffer against supply shocks**. Emergency reserves provide critical buffers when fuel disruptions threaten essential services, supporting critical mobility and enabling backup generators to sustain hospitals, water utilities, telecommunications and emergency services during prolonged outages. Legal frameworks must mandate minimum reserves with clear ownership, custody arrangements, and release protocols that are established before crises occur.

7. **Standardise and stockpile critical equipment**. Equipment standardisation dramatically accelerates repair timelines by enabling the rapid deployment of compatible components, while strategic and tracked stockpiles ensure availability during emergencies. Long-term manufacturer agreements with emergency priority access enhance the security of supplies for critical infrastructure.

8. **Treat data as a strategic asset and continue its collection during emergencies**. Crises disrupt data collection precisely when information becomes most critical for assessing damage, prioritising restoration, evaluating response effectiveness, and conveying both short-and medium-term needs to partners. Emergency legislation must ensure continuation of critical data flows through both technical measures and clear reporting responsibilities.

9. **Embed cyber resilience into all aspects of system planning and operations**. As distributed architectures create thousands of potential entry points, layered security with strict network segmentation, continuous monitoring, and international threat intelligence sharing becomes essential. Ukraine's successful prevention of attacks targeting millions demonstrates the value of combining secure-by-design principles, prompt cyber incident response and rapid coordination among stakeholders.

10. **Build mechanisms for cross-border cooperation.** Countries often cannot respond to high-impact events alone. International cooperation enables the necessary distribution of equipment, expertise and resources. Mutual assistance agreements with clear obligations and cost-sharing, established in advance rather than during crises, enable rapid deployment under established protocols and prevent months-long delays.

The growing imperative of energy system resilience

Energy system resilience has become paramount in managing the myriad of risks, ranging from weather disruptions to geopolitical uncertainty. **Energy security** encompasses both the long- and short-term dimensions of uninterrupted energy availability, at affordable prices and under all conditions. The long-term dimension focuses on adequacy – meeting demand under normal operations through infrastructure investment and diverse sources of energy supply. The short-term dimension embeds **resilience** – managing events that exceed standard planning conditions. Resilience includes the ability to prepare for disruptive events, adapt to gradual changes in the physical environment, continue operating when exposed to shocks (e.g. extreme and severe weather events, cyberattacks or physical attacks) and resume operations quickly after disruptions. Because threats cannot always be predicted or prevented, energy systems must be designed for rapid response: isolating affected components and restoring services swiftly when disruptions occur.

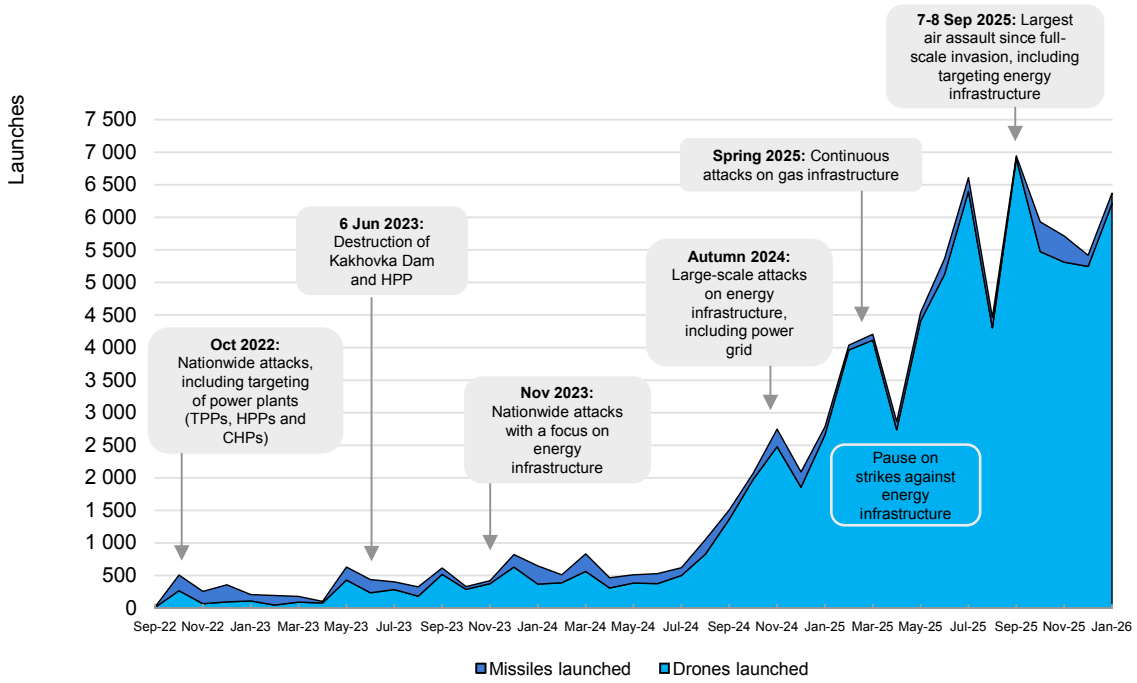
Addressing resilience requires moving beyond purely preventive approaches to embrace adaptive strategies. These include integrating resilience into system planning, deploying robust monitoring and early warning systems, building operational flexibility to reroute energy flows, and establishing redundant infrastructure that enables quick recovery. This document provides policy makers and regulators with a toolkit of measures that can be selected and adapted to national circumstances and risk profiles, considering both the costs and benefits.[1]

[1]The benefits of resilience are much more difficult to measure than the costs. A CERRE publication suggests measuring resilience benefits by comparing system performance during extreme events against scenarios with and without specific investments. Such assessments may use metrics like Value of Lost Load (VoLL) that capture direct and indirect costs of disruptions. Benefits are calculated by multiplying avoided losses by event probability – essentially quantifying the insurance value against catastrophic damages from low-probability, high-impact events.

Ukraine: An extreme test of energy system resilience

Since the beginning of the full-scale invasion of Ukraine by the Russian Federation (hereafter “Russia”) in 2022, Ukraine's energy system has endured systematic attacks, creating an unprecedented stress test of its resilience. According to the Ministry of Energy, Ukraine’s energy infrastructure was attacked 4 500 times in 2025 alone, involving 1 800 missiles and 50 000 drones. After four years of war, Russia has destroyed, occupied or damaged infrastructure across Ukraine’s energy sector, including oil refineries, oil and gas storage facilities, thermal, hydroelectric and nuclear power plants, as well as gas, heating and electricity distribution networks. Russia has leveraged its detailed knowledge of Ukraine's energy system – inherited from the Soviet era – to target assets whose failure creates the greatest impact, particularly electrical substations that are vital for connecting key generators, and which are costly to repair or replace.

Monthly Russian attacks on Ukraine per weapon type, September 2022 to January 2026



Sources: IEA analysis based on the dataset available on kaggle (Massive Missile Attacks on Ukraine - Data Review 2026), on drone and missile attacks by the Ukrainian Ministry of Defence and the Ukrainian Government.

While no part of Ukraine's energy sector has been left unscathed, the power system has been hit especially hard, resulting in electricity shortages and frequent blackouts. In 2024 alone, Ukraine lost 9 gigawatts (GW) of power generation capacity – equivalent to half of its peak winter electricity consumption. The situation worsened in 2025: Ukrainian households endured 1 951 hours of power outages – roughly 20% of the year – as a result of intensified Russian strikes on energy infrastructure, compounded by an exceptionally harsh winter. Blackouts during severe, sub-zero conditions were particularly devastating. Southeastern Ukraine continues to experience extensive blackouts and extreme power shortages in early 2026. As of mid-January, Ukraine's electricity demand reached 18 GW while the power system's daily capacity stood at roughly 11 GW.

While Ukraine's air defences provide a measure of protection, the scale of the disruption underscores the strategic importance of the country's energy sector and the persistent vulnerability of electricity supply. Every restored megawatt is also vulnerable to a second strike. Despite these challenges, Ukraine continues to provide many essential services while developing a new resilience architecture based on decentralised electricity and heat generation, microgrids and underground control systems.

System resilience challenges: Why Ukraine's experience matters

The strategies Ukraine is adopting to enhance energy system resilience have been forged under extreme and tragic conditions. The scale and systematic nature of the attacks on the country's energy infrastructure – compounded by severe winter conditions – represent an extreme challenge. Nonetheless, they offer insights and lessons that transcend the specifics of the war in Ukraine, and can apply in diverse contexts to countries facing extreme weather events, unexpected system failures and malicious attacks.

Extreme and severe weather events are becoming increasingly disruptive to electricity systems worldwide. In 2023 alone, power cuts due to weather impacted more than 210 million households.[2] Storms and floods together affected 95 million households, while heatwaves and cold spells cut power to over 75 million. Roughly 85% of these incidents were linked to grid damage or pre-emptive shutoffs, underscoring how vulnerable electricity infrastructures are to extreme and severe climate.

[2] The stats were based on 300 tracked events of outages (IEA [2025], World Energy Outlook).

Ukraine's ongoing transformation illustrates how distributed resources, energy storage and digital grid technologies can enhance both security and resilience. These solutions enable energy systems to withstand shocks, recover faster, and operate with greater confidence in an uncertain world.

Lessons for energy system resilience

Ukraine's accelerated energy system transformation, borne from necessity, provides 10 critical lessons for energy decision makers across the globe.

Lesson 1: Put resilience at the centre of energy system planning

Power systems designed for resilience can withstand disruption, recover more quickly and return to normal operation during extreme events, justifying investments by avoiding the catastrophic societal costs of prolonged outages.[3] This means targeting rapid service restoration after high-impact events (e.g. extreme and severe weather, physical attacks) – which may be rare, but which risk catastrophic consequences – alongside system-wide performance measures for routine events.[4] This may require backup resources or mobile, temporary assets when faced with time-consuming repairs of the core infrastructure.

Funding investments in resilience presents challenges, but it is essential given evolving threats. Energy-sector actors need appropriate regulatory frameworks to secure the resources needed for such measures, particularly given the already considerable investment demands of the energy transition and the importance policy makers place on affordability. But treating resilience investments as optional or deferrable is increasingly risky in today's threat environment.

Integrating resilience considerations at the planning phase reduces overall costs compared to retrofitting systems, and it should not slow planning processes if incorporated systematically. The key is achieving reasonable cost-benefit balance: rigorous assessment should justify investments through quantified avoided losses, while planning frameworks should streamline, rather than complicate, decision making. For example, Ofgem, the regulator for the electricity and gas markets in the United Kingdom, is considering including resilience measures – such as cyber resilience – in base cost allowances for system operators, promoting a mindset in which resilience is treated as a business-as-usual rather than an exceptional expenditure.

[3] A CERRE report introduces the "resilience trapezoid" framework that visualises how resilient systems exhibit steeper recovery slopes compared to conventional systems during extreme events, using metrics like Value of Lost Load (VoLL) to monetise the benefits of faster restoration.
[4] Typically, system average interruption duration and frequency indices (SAIDI and SAIFI).

Ukraine's experience and lessons learned

Ukraine's pre-war system lacked resilience-focused planning – a gap that is now being addressed under extreme duress. The Soviet-era electricity grid benefitted from ample generation reserve margins and a robust, highly integrated transmission network, but Russia's systematic attacks on generation facilities and transmission substations have exposed critical vulnerabilities. This centralised system, which exhibited single points of failure,[5] was not designed to sustain prolonged islanded operation when grid segments were isolated, and offered only limited backup capacity for end users.

Ukraine is now transforming its system architecture out of necessity. But rather than simply rebuilding what was destroyed, Ukraine is pursuing a three-pronged solution: **distributed generation to avoid single points of failure**, **energy storage for supply continuity** and **modular infrastructure for rapid deployment** (see also Lesson 5). Since the country remains heavily reliant on its remaining nuclear facilities – which cannot be targeted in the same way as other thermal assets – the deployment of distributed resources enhances overall system resilience.

Distributed solar provides critical backup during grid disruptions, albeit with varying effectiveness depending on the season. Ukraine has rapidly deployed an estimated 1.5 GW of rooftop solar capacity since the invasion began. Behind-the-meter installations that can operate in islanded mode provide critical backup during grid disruptions. In the city of Zhytomyr, for instance, a hospital combines solar power with 30 kWh batteries to keep its intensive care unit and surgical department running for several hours during blackouts. This approach offers resilience against both intentional attacks and system failures.

Energy storage has also become central to Ukraine's resilience strategy. Despite attacks on hydro reservoirs, storage capacity is expanding. In 2025, DTEK, Ukraine's largest private energy company, together with Fluence, a global energy storage provider, built a 200 MW/400 MWh storage system, distributed across six sites, that is capable of powering 600 000 homes for two hours. Ranking among Europe's top three facilities by energy capacity,[6] this installation stabilises the power system, reduces blackout risks and increases resilience under wartime conditions. Despite the ongoing conflict, the EUR 125 million project was completed in six months, though planning began years earlier – a standard timeline for European battery projects.

[5] A single point of failure is a non-redundant component, element, or path in an electricity system whose malfunction or loss would cause the entire system (or a relevant part of it) to fail.
[6] Comparable large-scale battery energy storage systems include: 300 MW/600 MWh in the United Kingdom; 124 MW/496 MWh in Bulgaria and 137.5 MW/275 MWh in Germany.

Ukraine's experience holds universal lessons, though the optimal approach varies by context and asset criticality. Legacy systems designed for different priorities can be reconfigured for resilience through deliberate planning that prioritises redundancy, distribution and modularity over pure efficiency or lowest cost. But planning proactively for resilience – before systems are under attack – allows for more systematic, cost-effective approaches.

Practical recommendations

- **Integrate resilience into system planning** by mandating holistic risk and resilience assessments alongside traditional reliability studies. Planning processes must explicitly evaluate how systems perform under high-impact, low-probability events, not just normal operating conditions.
- **Adopt resilient-by-design specifications** requiring enhanced redundancy for critical infrastructure, backup power for essential services, and decentralised modular architectures (see also Lesson 5) that enable managed degradation rather than cascading failures. Integrating resilience at the design phase reduces overall costs and implementation complexity compared to retrofitting.
- **Reform regulatory frameworks** to treat resilience as a legitimate cost and incentivise resilient design. Evaluate the cost-effectiveness of resilience spending proposals, balancing long-term security benefits against affordability and impact. Resilience measures should also be calibrated to the specific threats, recognising that proportionate responses vary significantly across the threat spectrum.
- **Establish standardised resilience metrics** to assess both preparedness and performance. Track whether critical infrastructure has alternative supply routes and can operate independently during grid disruptions – identifying weaknesses before they lead to service interruptions. Measure how systems actually perform during events, through average recovery time by outage severity and critical service continuity rates.

International examples of resilience planning and investment

Restoration speed is a key priority in national resilience frameworks. In **Italy**, the transmission operator Terna uses risk-based methodology, including specific recovery actions to reduce line restoration times, while the regulator ARERA requires distribution operators to publish plans addressing both the ability to withstand events and restore standard operations afterward. The **United Kingdom** requires resilience strategies to include workforce capacity and asset

health, ensuring recovery is not hampered by a lack of engineering staff or spare parts during emergencies.

Several countries have implemented specific regulatory mechanisms to support resilience investments. In the United Kingdom, the energy regulator Ofgem requires Distribution System Operators (DSOs) to include comprehensive climate resilience strategies in their business plans. Italy's regulator ARERA introduced incentive-based regulation requiring DSOs to publish prioritised three-year plans defending networks against specific hazards like ice, heatwaves and flooding, supported by cost-benefit analyses.

Experience demonstrates that climate-resilient energy systems consistently deliver benefits that exceed costs. The IEA's 2022 report on climate for energy security provides a comprehensive methodology for conducting cost-benefit analysis of climate adaptation measures, considering both direct energy system impacts and wider economic effects. In Africa and Asia, net benefits from flood resilience in the power sector are projected to reach USD 1 trillion by 2050, with benefits exceeding costs by a factor of 3 to 8 in Asia and 11 to 15 in Africa. Technical hardening measures have proven highly cost-effective: increasing a hydropower plant's spillway capacity typically adds only 3% to project costs but reduces damage probability by 50%. Similarly, wind farm strengthening adds 5% to costs but halves the probability of cyclone damage. In Florida, smart grid infrastructure deployed after Hurricane Irma in 2017 saved nearly USD 1.7 billion in avoided customer interruption costs, demonstrating the operational value of resilience investments.

Lesson 2: Implement physical hardening and defence measures

Physical hardening protects energy infrastructure from both intentional threats and natural hazards through comprehensive protection strategies. While threat sources vary – targeted attacks, extreme and severe weather, seismic events or accidental impacts – many hardening techniques strengthen systems across threat vectors, generating collateral benefits beyond their primary purpose. Even where military threats are low, countries should consider hardening energy infrastructure that faces recurring natural hazards (such as hurricanes, wildfires or floods), lies in seismically active zones, or is deemed critical to national security (Box in Lesson 1).

Effective hardening relies on both pre-planned infrastructure and rapid-deployment capabilities. The most robust protections must be built in from the start. However, lower-tier measures can rely on stockpiled equipment and clear deployment strategies rather than permanent infrastructure. Physical protections

such as sandbags, gabions and protective barriers can address both extreme weather and security threats, but they require sufficient reserves and clear protocols for rapid deployment to priority assets.

Similarly, anti-drone systems and electronic countermeasures require advance procurement and trained operators, with deployment focused on protecting critical infrastructure rather than achieving universal coverage. This approach – combining permanent protections with deployable measures – provides cost-effective flexibility to address evolving threats.

Ukraine's experience and lessons learned

In response to the full-scale invasion and escalating Russian attacks, Ukraine has worked to deploy a **three-level protection framework** for energy infrastructure with support from the North Atlantic Treaty Organisation (NATO). This approach addresses immediate vulnerabilities while building long-term resilience across electricity, gas and oil infrastructure. For Ukraine, however, air defence plays a key role in protecting energy infrastructure, complementing passive protection measures. Russia's more recent tactic of striking energy infrastructure twice in quick succession ("double tapping") demonstrates the limits of relying on physical hardening alone.

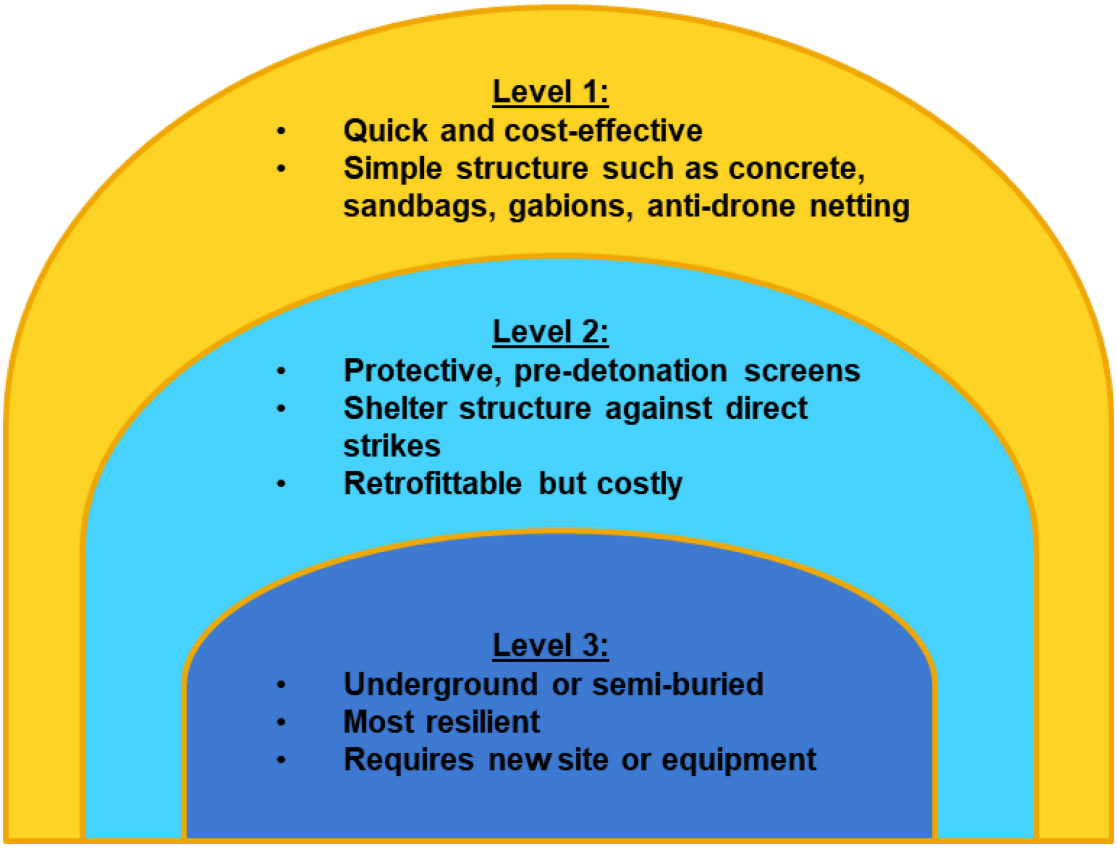
Level 1 protection uses sandbags, gabions, reinforced concrete, nets and other physical barriers to shield critical equipment from debris and indirect strikes. These measures can be deployed quickly and cheaply, limiting damage from nearby missile or drone strikes. Ukraine has made Level 1 measures the foundation of its infrastructure defence.

Level 2 protection combines hardened physical barriers, including reinforced concrete that surround and shield key equipment, with electronic countermeasures against direct drone hits. While more costly to implement, this multi-layered approach has helped preserve critical infrastructure despite constant attacks. Testing shows both Level 1 and Level 2 protections reduce damage from indirect hits by approximately 50%.

Level 3 integrates hardening at the design stage, locating facilities underground or within reinforced shelters capable of surviving direct missile strikes. So far, Ukraine's deployment of Level 3 measures has been limited. Retrofitting existing assets to this standard is extremely difficult, costly and slow to build. Selective hardening offers a practical alternative. Reinforcing or burying critical elements of facilities like hydropower plants can provide significant protection without requiring full underground construction. This reinforces a key infrastructure planning principle (Lesson 1): the highest levels of resilience are best incorporated when new assets are first built, rather than retrofitting existing systems. Ukraine's implementation priorities focus on several key areas: anti-drone netting and

electronic countermeasures near critical substations, placing vulnerable equipment underground, and reinforced transformer protection with blast-resistant barriers. Additional measures include camouflage and concealment of critical facilities and deliberate reduction of publicly available information about infrastructure locations. These defensive measures can also be applied to oil and gas production facilities, storage sites and transport infrastructure.

Three levels of physical protection of energy infrastructure



Source: IEA analysis based on information shared by NATO Energy Security Centre of Excellence, the Critical Infrastructure Protection Department, Ministry of Development of Communities and Territories of Ukraine, and the Ministry of Defence of the United Kingdom.

Security protections also improve extreme weather resilience and operational safety. Underground cables installed for security also avoid the need for thermal de-rating during summer heat, unlike overhead lines. Structural reinforcements designed to withstand explosions also improve seismic resistance and protect against heavy snow loads. These co-benefits strengthen the economic case for physical hardening by addressing multiple risks simultaneously, unlike single-purpose protections.

Practical recommendations

- **Establish regulatory frameworks requiring key energy stakeholders to conduct regular vulnerability assessments** across all physical threats: climate extremes, seismic events and deliberate attacks. Provide clear cost-recovery mechanisms for necessary hardening investments.
- **Establish minimum baseline standards for protecting all energy assets** and implement tiered defences proportionate to threat levels. Begin with systematic deployment of basic site protections across all facilities: controlled access, perimeter fencing, physical barriers and video surveillance. The January 2026 attacks on Germany's power grid demonstrated that energy infrastructure remains exposed to deliberate sabotage, even in peacetime.
- **Design for multi-purpose protection.** Co-benefits strengthen the economic case: measures protecting against one threat often enhance resilience to others. Underground cables in storm-prone areas, for example, defend against both extreme weather and airstrikes.

Lesson 3: Build comprehensive emergency response capabilities that cover multiple threat scenarios

Effective emergency response requires advance preparation for a range of high-impact events. This includes developing plans and protocols, maintaining trained teams with technical expertise, stockpiling specialised equipment and establishing co-ordination mechanisms – all validated through periodic exercises. Resilient systems must prepare not only for familiar threats from recent experience, but also for less likely scenarios such as hybrid attacks, cascading cross-sector infrastructure failures and extreme and severe weather events exceeding historical severity.

Ukraine's experience and lessons learned

Ukraine has transformed emergency response from theory to practice under extreme pressure, revealing essential resilience factors. The most critical capability proved to be rapid restoration while under attack: repair teams had to restore damaged facilities faster than ongoing attacks could destroy them. This required substantial evolution of pre-war practices.

Pre-positioned resources and in-house expertise have become critical enablers as well. When supply chains were disrupted, having critical equipment and materials on-site made it possible for operations to continue where they might otherwise have ceased. Ukraine's wartime experience reveals the importance of retaining technical and engineering personnel in-house, which goes against the recent peacetime trend of outsourcing maintenance. This ensures immediate repair capacity under fire, with restoration speeds that can outpace destruction

rates. Training personnel to handle multiple roles also provided flexibility when specialists were unavailable. In Ukraine's case, energy workers face acute danger during emergency repairs, particularly as Russia has stepped up double-tap strikes. Finding ways to respond flexibly while also working to protect energy workers has been a complex balancing act.

Ukraine adopted several measures to manage unprecedented electricity shortfalls. Public co-operation in reducing electricity use proved vital, driven by public awareness campaigns and incentive programs that reduced stress on the power grid during vulnerable periods. However, much of the demand reduction was involuntary – factories were destroyed by attacks or shuttered due to wartime conditions. Ukraine also developed systems for managing rolling blackouts, including hourly shutdown schedules and power limitation protocols. Authorities also strengthened civil-military co-ordination to accelerate repairs during attacks and improve preparedness for future disruptions.

Meanwhile, legal frameworks needed to be quickly adapted. Wartime experience revealed the inadequacy of improvised crisis response. Ukraine had to rapidly enact or modify laws enabling emergency procurement, international aid distribution and expedited grid interconnection procedures. The government also streamlined import procedures for distributed-generation equipment. In November 2025, Ukraine's Cabinet of Ministers authorised energy companies to establish air defence units in co-ordination with the Armed Forces – a striking example of wartime governance adaptation.

Often, planning assumptions failed to account for extreme scenarios. Ukraine's pre-war plans for single-point failures or brief outages proved inadequate against sustained attacks. In the early days of the 2022 invasion, strikes on storage terminals and refineries caused critical fuel shortages. However, the government was able to mitigate the impact by deregulating fuel markets, which enabled private suppliers to fill supply gaps more quickly. Ukraine's pre-war planning did not anticipate prolonged, co-ordinated attacks on multiple supply chain elements simultaneously.

Practical recommendations

- **Develop comprehensive emergency response plans** that address co-ordinated infrastructure attacks, extreme and severe weather events, combined cyber and physical threats, as well as cascading failures across inter-dependent systems. Planning must anticipate novel threats beyond historical experience, including low-probability, high-consequence scenarios. The Australian Energy Market Commission's system security rule determinations offer a model for this approach. Predefined escalation protocols and decision-making frameworks enable faster response by

eliminating the need for prolonged deliberation in a crisis. Regular scenario exercises build familiarity with emergency procedures that are critical during actual crises.

- **Establish command structures that enable real-time situational awareness and rapid identification of response options.** Formalise roles and responsibilities among authorities (at municipal, regional and federal levels) and co-ordinate expertise across sectors (e.g. energy, defence, cybersecurity). Establish a crisis-management team with the right skills to execute the plans.
- **Establish legal and operational frameworks in advance**. Pre-authorise emergency procurement procedures, expedited connection requirements for backup generation, and streamlined decision-making authority. Define restoration priorities and procedures for accepting international assistance. Develop risk-preparedness plans that are aligned with frameworks like the European Union Risk Preparedness Regulation and identify scenarios, responses and civilian-military co-ordination mechanisms (see Box on Sweden's total defence concept).
- **Develop demand-restraint capabilities as operational tools.** Establish demand-reduction frameworks that combine public awareness campaigns, behavioural incentives and priority allocation systems. Manage demand to balance supply shortages, prioritising voluntary reduction and implementing load shedding when necessary.
- **Maintain in-house technical capacity and conduct regular preparedness exercises**. Retain skilled personnel rather than outsourcing to enable rapid emergency response. Conduct regular tabletop exercises and field drills with all stakeholders, including local authorities, government agencies and international partners. Update threat assessments regularly as conditions evolve.

Sweden's Total Defence

Sweden has developed Total Defence (*Totalförsvaret*), a comprehensive whole-of-society approach to national security that integrates both military and civil defence capabilities. This concept was originally conceived during the Cold War but was largely dormant after 1991. It has been revitalised since 2015 due to the deteriorating security situation in Europe, particularly following Russia's invasion of Crimea.

Energy supply is explicitly identified as one of the **civil preparedness priorities** within Sweden's Total Defence framework. The legislation, "Totalförsvaret 2021-

2025," singles out energy supply as one of the most important societal functions requiring enhanced resilience.

Sweden's Total Defence must be capable of resisting serious disturbances to societal functioning for three months, during which time the country must be able to defend itself and endure hardships with limited external support. In the initial two weeks of a war, civil agencies and the private sector are encouraged to keep vital services – including food, water and telecommunications – running primarily from their own resources. Citizens are encouraged to have household readiness to survive without state assistance for at least one week, and shelters must be prepared for use within 48 hours during crisis escalation or armed conflict.

Total Defence consists of two main components: military defence and civil defence. It mobilises actors at every level: national (parliament and government agencies), municipal authorities, private companies, volunteer organisations, and individual citizens aged 16 to 70. The concept is based on the principle that when the government orders the highest state of alert, all functions of society are engaged in the defence effort, both military and civilian.

Energy security and defence priorities can sometimes conflict. In August 2025, Sweden cancelled 13 offshore wind projects (almost 32 GW of capacity) over potential interference with airborne and undersea detection systems, sparking debate about the balance between renewable energy development and defence capabilities.

Lesson 4: Ensure effective emergency communication mechanisms to reach citizens

Effective public communication during crises requires redundant channels that function when primary infrastructure fails. While many countries have adopted text message (SMS) alert systems, emergencies often disrupt the telecommunications infrastructure on which these systems rely. Resilient emergency communication combines digital systems with analog backups that function when cellular networks fail.

Ukraine's experience and lessons learned

Ukraine learned that **no one communication channel can be relied upon during a crisis.** The Ukrainian government has traditionally used digital channels for emergency communication with citizens. But when Russian attacks targeted the country's telecommunications infrastructure, these systems were rendered unreliable, forcing a rapid shift to multi-channel approaches. The lesson was clear: digital systems offer convenience, speed and precision, but traditional technologies provide resilience when modern infrastructure fails.

Multi-channel systems are critical for maintaining public communication. Ukraine developed rolling blackout communication systems that combined mobile applications, social media and traditional media. The country's air raid alert system integrates sirens, mobile applications and push notifications, all co-ordinated by the State Emergency Service, with real-time inputs from civil defence and military authorities. Alerts specify the type and trajectory of incoming strikes, impact locations, infrastructure damage and radiation levels. Electricity providers use targeted messages helping citizens navigate rolling blackouts and power-reduction schedules.

Backup methods became critical when digital infrastructure failed. Radio broadcasts reached populations without electricity through battery-powered or hand-crank radios. Sirens provided area-wide alerts without the need for individual receivers. Local community staff reached out personally to populations without smartphones or during network disruptions, and physical signs were posted at critical locations. Popular messaging applications and social media channels also disseminated critical information quickly, while also combating disinformation.

Credibility requires transparency and consistency. Critical success factors included consistent messaging transparency about uncertainty, and co-ordination across government, utilities and local authorities. Ukraine's experience also demonstrates that regular in-person briefings from energy authorities complement digital communications, providing context and building trust during prolonged crises. Supervisory agencies can publish practical guidance for staying warm and safe during power outages, for example. Municipal authorities can give regular updates on restoration progress to help communities and businesses plan around extended power and heating disruptions. In addition, local communities have come together to establish unofficial warming hubs in cafes, while households have strengthened their resilience by installing solar panels and portable backup generators.

Practical recommendations

- **Establish multi-layered communication systems** where backup channels function independently of primary infrastructure. Traditional AM/FM radio reaches populations without electricity, while sirens provide area-wide warnings without the need for dedicated devices. Community networks leverage local leaders, and physical signage identifies critical locations. Mobile SMS alerts are still valuable, but they should never be the sole communication channel in a crisis.
- **Deploy crisis applications while leveraging existing platforms.** Use dedicated applications for targeted alerts (e.g. rolling blackout schedules) while also utilising social media and messaging applications to share

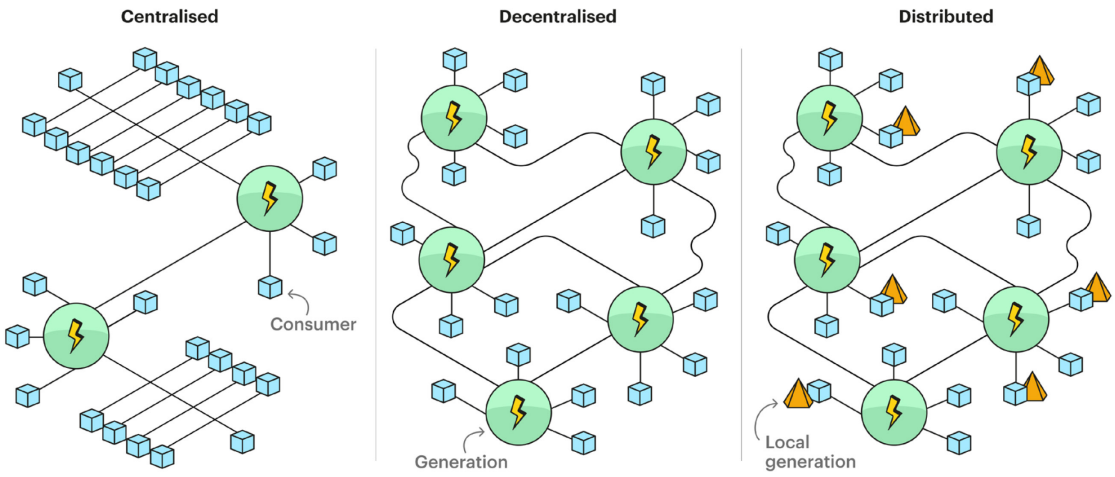
information widely and quickly. Multiple channels ensure redundancy when individual platforms fail or reach different population segments.

- **Build credibility through regular practice and transparency.** Test systems with actual notifications, be transparent about limitations, educate the public on alert interpretation, and use emergency channels only for genuine threats to prevent alert fatigue. Provide regular in-person briefings during extended crises, not just digital updates.
- **Provide clear, actionable guidance.** Specify what people should do, include realistic timing while acknowledging uncertainty. Publish practical guidance, including safe heating methods during outages and locations of warming centres and charging stations.

Lesson 5: Leverage decentralisation and distributed generation as a strategic security asset

Decentralised system architectures reduce vulnerability to single points of failure, creating flexible and adaptable energy systems. Distributed assets are inherently harder to target and easier to restore or rebuild when damaged. The vulnerability differential between centralised and distributed generation in Ukraine demonstrates that decentralisation is not merely an energy transition strategy: it is a fundamental imperative for energy security and resilience. Distributed resources can also restart the system after regional or local blackouts, as demonstrated by the Distributed ReStart project in the United Kingdom.

Decentralised and distributed system architectures



IEA. CC BY 4.0

Note: **Centralised systems** rely on few large supply nodes, creating single points of failure. **Decentralised systems** distribute supply across multiple nodes, reducing vulnerability. **Distributed systems** additionally provide backup resources at demand nodes, enabling continued operation during network disruptions.

Ukraine's experience and lessons learned

Ukraine has strategically embraced decentralisation as a core resilience response. Russia's systematic attacks on centralised generation facilities since 2022 convinced Ukraine that rebuilding the same vulnerable architecture would perpetuate existing risks. As a result, the country is moving to a system that distributes generation capacity across multiple, smaller nodes. The IEA's December 2024 report on empowering Ukraine through a decentralised electricity system describes this strategic shift, emphasising how distributed resources can speed crisis response as well as promote long-term system resilience. The strategy centres on deploying distributed solar, battery storage and microgrids, enabled by regulatory reforms that accelerate deployment. Ukraine has also deployed mobile gas turbines and diesel generators to maintain emergency backup power. It has also provided liquid petroleum gas (LPG) heating units as alternatives to electric heat during blackouts. Simplified definitions and classifications of distributed energy resources have also helped to speed deployment and grid integration.

While not immune to disruption, distributed resources have proven significantly more resilient: More than half of Ukraine's centralised generation capacity has been damaged or destroyed, compared to just 7% of distributed generation. Distributed resources are more difficult and costly for attackers to locate – especially recently built capacity that does not appear on legacy maps. Distributed generation assets can also be repaired and rebuilt more quickly than centralised generation facilities. This demonstrates how dispersing assets geographically inherently provides protection that hardening measures alone cannot achieve for concentrated facilities. Distributed resources have enabled Ukraine to maintain critical services when centralised infrastructure has failed, proving their value as a strategic security infrastructure.

Recovery dynamics favour distributed generation. Protection and restoration of centralised facilities necessitate substantial investments and, in the case of nuclear plants, also require specific, time-consuming safety procedures before restart. By contrast, damaged solar photovoltaic (PV) or battery modules can be quickly taken offline and replaced without affecting other units, connected systems, or posing significant environmental or public safety risks. This modularity applies to systems ranging from rooftop installations to utility-scale solar and battery facilities. Decentralisation is also effective for heating. The city of Kharkiv exemplified this approach in the winter of 2025-2026, using heat pumps, cogeneration units and mobile boiler houses to maintain heating after centralised systems failed. In January 2026, despite its proximity to the front line, Kharkiv was better prepared than cities like Kyiv, where energy stabilisation measures struggled to cope with recurring attacks and outages, leaving more than 5 500 residential buildings without heat.

Ukraine has prioritised decentralisation throughout the crisis. Recently, the Ministry of Energy allocated almost UAH 21 billion (EUR 420 million) to strengthen energy security. While the bulk of funding (48%) went to reconstructing hydroelectric power plants, decentralised power generation became a strategic priority for ensuring uninterrupted power for critical services. The primary objective for critical infrastructure is ensuring physical protection against disruptions while maintaining the capacity for rapid recovery. In 2024, the government presented an Internal Resilience Plan that identified energy as a key sector and introduced measures to establish Ukraine as a regional energy hub, while promoting sustainable resource use.

The rapid deployment of distributed generation helped Ukraine sustain critical services. New legislation accelerated the transformation by fast-tracking approvals for local generation units at multiple sites across the network. Just a few months after Ukraine approved its Distributed Generation Development Strategy, cogeneration facilities were installed in 32 cities. A further 83 plants were connected to the grid and 82 more were delivered for installation. In January 2026, the government launched a state aid programme targeting the purchase of autonomous power sources for citizens and businesses, allocating almost EUR 16 million.

Medical facilities benefit from the complementarity of solar systems and diesel generators during outages. Traditional diesel generators pose challenges: fuel is expensive to stockpile and can pose a fire hazard. There is also the risk of supply disruptions. This has prompted hospitals and clinics to shift to local renewable generation for backup power. Through its Ukraine Energy Support Fund, the European Energy Community has facilitated solar PV installation at 83 hospitals across Ukraine. Energy companies from the United Kingdom have also supported projects like the Vinnytsia Regional Children's Clinical Hospital, where solar power units have ensured uninterrupted paediatric care during blackouts. In the Vinnystia region, co-operation between the local utility and a small hydropower operator led to the creation of five microgrids, capable of supplying power to neighbouring settlements during complete blackouts.

Technology has facilitated system decentralisation. Ukraine's experience highlighted critical technology requirements: microgrid systems combining distributed solar with mobile small gas turbines and battery storage capable of operating independently for at least four hours to sustain households and businesses during outages. Distributed solar capacity grew rapidly and was often deployed in small-scale configurations operating independently from the main grid. Intelligent grid-management platforms, using real-time data and artificial intelligence (AI)-enabled decision making, became essential for optimising power flows, co-ordinating distributed resources and maintaining stability as power architectures grew more decentralised and digitalised.

Legislative support was essential. With support from the United Nations Development Programme's Green Energy Recovery Programme, Ukraine's parliament adopted laws that simplified regulatory procedures and bolstered investment in distributed energy resources. Dedicated legislation defined key terminology for demand management, demand response, microgrids and island mode operation of generation units. The Distributed Generation Development Strategy recognised the fundamental role of these assets, aiming to increase installed local generation and storage capacity, modernise network infrastructure through smart grids and digitalisation, and facilitate construction by attracting private and foreign investment.

Decentralisation principles extend beyond electricity. Before the full-scale invasion, Ukraine's oil products supply chain relied on emergency reserves that were held in large, centralised storage terminals. When these were targeted, alongside refineries and logistics hubs, the impact was immediate and severe. The destruction of even a few large storage facilities decimated fuel stockpiles and disrupted nationwide distribution. Holding emergency reserves in geographically distributed storage facilities would have reduced the risk of severe shortages and ensured that reserves remained accessible when they were most needed.

Practical recommendations

- **Prioritise distributed energy resources as strategic security assets**. Deploy distributed generation (e.g. solar, wind, battery storage) and microgrid architectures to localise generation and enable islanding of critical loads. Mobile gas turbines and fuel generators can serve as emergency backups during acute crises. Geographic distribution of assets reduces the risk of single-point failure and sustains essential services during attacks or system disruptions.
- **Establish enabling legislative and regulatory frameworks**. Remove regulatory barriers and create clear interconnection and operational rules for distributed generation, storage, microgrids and demand response. Streamline permitting to accelerate deployment and reduce investor risk. Mandate training and capacity-building to ensure qualified personnel can operate and scale decentralised systems.
- **Deploy intelligent grid management platforms**. Use real-time data and AI-enabled decision making to optimise power flows, co-ordinate distributed resources and maintain stability and digital security as system architecture becomes increasingly decentralised and digitalised.
- **Extend decentralisation principles beyond electricity**. Consider interdependencies among subsectors. Maintain strategic emergency reserves for oil and gas in geographically distributed storage facilities to reduce the risk of fuel shortages and ensure accessibility during crises.

How virtual power plants strengthened Puerto Rico's system after Hurricane Maria exposed the limits of a centralised grid

Puerto Rico's transformation into one of the world's largest virtual power plants (VPPs) demonstrates how co-ordinated distributed assets can evolve from individual backup systems into a national resilience backbone. In 2017, Hurricane Maria, a Category 5 hurricane, struck the United States territory of Puerto Rico, destroying transmission lines across the island. The disruption left 1.6 million customers without power and triggered the longest blackout in US history. Full restoration took nearly a year, exposing how vulnerable long-distance power delivery was to climate-driven disasters.

While Hurricane Maria revealed the extreme fragility of centralised infrastructure, rapid policy support enabled large-scale deployment of decentralised energy resources. By 2025, the island had aggregated more than 81 000 home batteries (out of 185 000 installed) into a VPP, delivering 20-30 MW of reliable capacity that reduced nighttime outages and peak-demand stress.

Puerto Rico expanded distributed solar and battery systems after Maria, backed by federal and local funding for rooftop solar, assistance programmes for low-income households, and grid upgrades. The Customer Battery Energy Sharing (CBES+) Programme accelerated home-battery adoption, offering USD 1.25/kWh for energy dispatched during emergencies. Since the summer of 2025, all battery-owning customers are automatically enrolled. Through CBES+, households share stored energy during emergencies via an automated dispatch network that is managed by aggregators. Emergency battery dispatch lasts two to four hours with day-ahead notice. Customers can set their own reserve levels or opt out.

The combination of distributed solar and storage has sharply improved resilience. During Hurricane Fiona in 2022, many homes equipped with solar and battery storage maintained power even as centralised systems failed. Compared with the pre-Maria era of days-long blackouts, the island now benefits from local energy autonomy. Research by the Brattle Group highlights how VPPs deliver "real reliability" by providing dispatchable capacity during critical periods.

This mirrors the experience in Ukraine, where repeated attacks on centralised infrastructure have driven communities to rely increasingly on rooftop solar, batteries and other distributed assets. Both cases demonstrate how distributed resources, when aggregated effectively, provide not just backup power, but co-ordinated system-level resilience.

Lesson 6: Maintain emergency oil stocks as a buffer against sudden supply shocks

Emergency oil reserves provide critical buffers when fuel disruptions threaten essential services and economic activity. At the national level, emergency stocks support key supply chains during fuel shortages and ensure that backup power generation can sustain critical services during prolonged outages. While not a permanent substitute for well-functioning oil markets, they are stabilisation tools that allow governments to temporarily maintain operations while supply chains are restored or reconfigured.

Ukraine’s experience and lessons learned

When war broke out, Ukraine was unprepared for fuel supply disruptions. The country had very limited oil stocks and lacked a comprehensive legislative framework mandating minimum reserve levels or detailing procedures for the emergency release of stocks. This gap proved costly when acute fuel shortages emerged after Russia's full-scale invasion.

Fuel shortages directly constrained critical operations. Russia's destruction of domestic refining capacity and the sudden loss of maritime import routes disrupted oil supply. Long queues formed at petrol stations, fuel purchases were rationed and prices rose sharply. These shortages directly constrained mobility for households and businesses, disrupted freight and agricultural activity, and complicated military logistics.

Limited stores of diesel threatened backup power. Although Ukraine has largely maintained adequate diesel supplies since its electricity infrastructure came under sustained attack, shortages immediately after Russia’s full-scale invasion threatened backup generators critical for hospitals, water utilities, telecommunications networks and local government services. While emergency reserves are not intended as long-term solutions, the impacts of the fuel shortages could have been mitigated earlier if Ukraine’s emergency reserves had been larger.

The legislative response acknowledged and addressed this critical gap. The government's adoption of minimum fuel reserve legislation in 2023 – requiring suppliers to maintain minimum reserve levels – reflects recognition of the importance of holding a sufficient level of emergency oil stocks. The law "On Minimum Reserves of Oil and Petroleum Products" establishes a framework that was absent at the outset of the invasion.

Practical recommendations

- **Establish explicit legal frameworks for fuel stockholding.** Ensure legislation provides legal authority to mandate minimum reserve levels commensurate with national risk profiles. Clearly determine which institutions are responsible for oversight and decision making related to reserve releases to reduce uncertainty and delays during crises.
- **Define ownership and custody arrangements clearly.** Specify whether emergency stocks are held directly by the state, delegated to designated agencies, or imposed as obligations on private market participants. Establish robust audit and reporting provisions to ensure reserves are maintained at legally mandated volumes and remain accessible when needed.
- **Calibrate reserve volumes to national vulnerabilities.** Consider factors including import dependency, domestic storage capacity, fuel requirements for critical services and potential disruption scenarios when determining appropriate reserve levels.
- **Ensure emergency stocks are physically accessible and operationally releasable.** This can be achieved by seeking to maintain an appropriate geographic distribution of storage sites while positioning stocks relatively close to likely demand centres and critical services. In addition, potential logistical bottlenecks should be assessed, including port capacity, pipeline and road dependencies, and the availability of trucking and rail transport. In parallel, the practical functioning of release mechanisms should be ensured by clarifying authorisation procedures, identifying priority users in advance and routinely testing release procedures.
- **Consider establishing emergency gas reserves.** As part of the emergency response, gas importers should work to ensure availability of sufficient supply and introduce measures to reduce vulnerability in a crisis.

Lesson 7: Standardise and stockpile critical equipment

Equipment heterogeneity creates acute supply chain vulnerabilities during emergencies. Technical standardisation of key components – such as transformers and substation equipment – can significantly accelerate repair timelines and reduce supply chain vulnerabilities. The level of standardisation must balance resilience benefits against innovation constraints, specific optimisation against interoperability, and cost considerations. Effective stockpiling of reserve equipment and spare parts is also essential, though compatibility remains an issue without standardisation.

Ukraine's experience and lessons learned

Non-standardised equipment significantly extended restoration timelines. Ukraine's replacement requirements exposed the consequences of equipment heterogeneity: sourcing compatible transformers, switchgear and control systems required extensive co-ordination, with each facility potentially needing custom specifications. This extended restoration timelines compared to what would have been possible with standardised spare deployment.

Compatible equipment enabled rapid installation when available. A fortunate exception illustrated the value of compatibility: Lithuania provided Ukraine with two 200 megavolt-ampere (MVA) autotransformers that could be installed immediately because both countries used the same voltage levels inherited from the Soviet Unified Power System/Integrated Power System (UPS/IPS) grid. These transformers became available when Lithuania replaced them in preparation for synchronisation with continental Europe in 2025. Other European Union border countries with Soviet-era legacy technology present similar opportunities.

Many donated transformers, switchgear, and protection relays faced compatibility issues that required additional engineering work, creating delays. Incompatibility with European Union grid standards and wider Soviet-era design challenges meant that integration required substantial retrofitting and modernisation beyond simply deploying surplus stock. Relaxing engineering standards to some degree can help balance deployment speed and resilience with longer-term system requirements. Defining acceptable deviations from established specifications in advance avoids difficult choices in times of stress.

Ongoing attacks compound stockpiling challenges. Stockpiling continues to be a challenge for Ukraine, particularly as Russian attacks damage and destroy dwindling global stocks of Soviet-era equipment. This highlights the dual challenge of maintaining emergency reserves while transitioning away from legacy technologies. In the meantime, Ukraine has created a national strategic transformer reserve. Considering where to locate strategic equipment (e.g. underground or in a neighbouring country) can enhance security and resilience, ensuring that it can be deployed when needed.

International experience demonstrates the benefits of proactive standardisation (see Box: Austria's standardisation initiative).

Practical recommendations

- **Develop equipment standardisation programmes.** Identify critical equipment types (e.g. transformers, circuit breakers, protection systems), define specifications considering future needs, ensure compatibility of

donations, co-ordinate across utilities to enable mutual support and plan transition timelines that account for decades-long implementation periods.

- **Maintain component inventories based on risk assessment**. Establish inventories of critical components, create regional stockpiling co-operatives to share resources (see also Lesson 10), define rapid deployment protocols, and rotate stocks to prevent degradation. Identify non-standard components and store these in dedicated warehouses for rapid deployment.
- **Ensure supply chain resilience.** Establish long-term agreements with manufacturers that guarantee priority access in emergencies. Develop domestic capacity for critical components where feasible, and monitor supply-chain developments, including significantly extended lead times (as was experienced in the wake of the Covid-19 pandemic).

Austria's transformer standardisation initiative

The experience of Austria's transmission system operator, Austrian Power Grid (APG), shows the benefits of proactive standardisation. APG reduced its transformer models to four standard designs, driven by procurement simplification (fewer specified types), operational uniformity (enabling the same transformer to be usable across different substations), and enhanced security of supply through reduced spare transformer variety.

APG's objective was to optimise and standardise large power transformer variants while adapting to changing logistics conditions with growing power demand. The strategy includes signing long-term framework agreements with manufacturers to secure needed volumes while maintaining consistency with technical specifications across contract cycles.

Challenges include managing technological evolution and the limited availability of specific components such as voltage regulation elements (on-load tap changers and automatic voltage regulators). APG addressed these issues by signing multiple procurement agreements to ensure supply continuity, demonstrating how standardisation requires sustained co-ordination between utilities and manufacturers.

Source: Austrian Power Grid.

Lesson 8: Treat data as a strategic asset and continue its collection during emergencies

Comprehensive, timely data about energy supply, demand and infrastructure are essential for decision making during normal operations as well as emergencies. Crises often disrupt data collection precisely when it is most needed. Taking proper precautions will ensure that data flows are maintained in any scenario.

Ukraine's experience and lessons learned

Ukraine instituted martial law as soon as the full-scale invasion began in 2022. This had implications for statistical data collection: all primary respondents were exempted from their reporting obligations until the state of emergency would be lifted. This had the unintended consequence of limiting the collection of data relevant for assessing the situation in the energy sector. An amendment allowing the resumption of statistical reporting was finally passed in June 2025. But as a result, disaggregated information on final energy consumption by industry, services and households were simply not available for more than three years, hindering medium- to long-term energy system analysis and modelling of reconstruction pathways.

Meanwhile, external (non-government) access to most short-term electricity data, such as flows and infrastructure, was limited, citing national security concerns. This significantly hindered external support as well as post-event analysis that could have supported the Ukrainian government's short-term decision making. The information embargo was also inconsistent: in some cases, data considered confidential by one stakeholder was publicly accessible elsewhere.

The scale of Russia's attacks on Ukraine's energy infrastructure revealed a gap: no system existed to systematically track damage to physical assets. While Ukraine established reporting mechanisms under pressure, such systems are far more effective when developed and tested during peacetime rather than improvised during crises.

The lack of data on hourly, daily and monthly energy flows created multiple challenges: it hindered systematic assessment of damage and prioritisation of restoration; it limited rigorous evaluation of response measures; it complicated efforts to quantify Ukraine's needs to international partners; and it obstructed the development of strategic documents such as the Energy Strategy and the National Energy and Climate Plan, both key pillars of European integration.

Experts at the Ministry of Energy, the Ministry of Economy and Ukrenergo, the state-owned transmission operator, had access to critical data and information that external stakeholders lacked. Although information was often shared on an ad-hoc and informal basis, this practice can sometimes prevent essential data from reaching all relevant stakeholders in an emergency.

Practical recommendations

- **Ensure continuity of both strategic and operational data collection during emergencies by removing legislative barriers and implementing practical measures**. Review legislation governing states of emergency (e.g., martial law) to ensure it does not block statistical energy data collection for

system planning and modelling. Implement technical measures (distributed IT infrastructure, automated procedures) and organisational measures (clear reporting responsibilities, backup channels) to preserve real-time operational data for grid management and immediate decision making, recognising that other constraints such as workforce availability and operational priorities may also affect data collection during crises.

- Establish **clear protocols for handling public vs. confidential data,** including classification levels, so that access restrictions on energy data are kept to a minimum.
- **Establish a framework for assessing damage to energy infrastructure and disruptions to data collection and data sharing** obligations towards the European Union's acquis relevant for (energy) statistics. This enables real-time situational awareness, rapid damage assessment and optimisation of resources.
- **Limit broad public access to critical infrastructure information**. While stakeholder engagement and transparency of market data improve overall system efficiency, sharing unnecessary critical infrastructure data and maps can have adverse effects when exploited by malicious actors.

Lesson 9: Embed cyber resilience into all aspects of energy system planning and operations

Modern energy systems face unprecedented cyber threats that require fundamental shifts in how resilience is conceived and implemented. Cyberattacks come in diverse forms, and can be part of hybrid campaigns that combine co-ordinated activities, including physical attacks, coercion and information manipulation. The transition to distributed architecture – where each decentralised unit, storage system and inverter represent a potential digital entry point – makes cyber resilience critical. Rapid deployment of distributed resources has often exceeded the pace at which robust cybersecurity frameworks could be established.

Ukraine's experience and lessons learned

Over the course of a decade, Ukraine has seen escalating cyber threats to its energy infrastructure. The BlackEnergy malware attacks in 2015 caused widespread outages, affecting hundreds of thousands of customers and marking the first confirmed cyberattack to successfully disrupt a power grid. The 2016 Industroyer malware campaign – which specifically targeted power grid control systems – demonstrated the sophistication of threats to electricity infrastructure.

The threat landscape intensified dramatically after Russia's full-scale invasion. It is estimated that Ukraine has suffered more than 660 cyber incidents since

January 2022, of which 38 specifically targeted the energy sector. These ranged from denial-of-service (DOS) attacks disrupting connectivity to Ukrainian energy companies, to website defacements, to direct targeting of critical electricity infrastructure. The February 2022 Viasat modem cyberattack, launched one hour before Russia's invasion, illustrates the cascading effects of cyberattacks: beyond disrupting Ukrainian telecommunications, a major German energy company lost remote monitoring access to more than 5 800 wind turbines, while outages affected tens of thousands of customers across France, Germany, Hungary, Greece, Italy and Poland.

Ukraine successfully prevented a major attack through rapid detection and international co-operation. In April 2022, a co-ordinated attack targeting several high-voltage electrical substations was discovered and prevented. Using malware similar to that deployed by the Sandworm APT group – officially identified as a Russian government-backed actor – the attack was scheduled to cut power to an estimated 2 million people. When Ukraine identified this threat, operational information, including malware samples and indicators of compromise, were immediately transferred to international partners and companies in the energy sector.

Ukraine's sustained resilience highlights critical success factors: Publicly reported cyberattacks on energy infrastructure since the invasion have not had decisive, destructive or strategically significant strategic effects. This resilience is built on defence in depth, with multiple security layers spanning physical, network and application domains. It relies on strict network segmentation separating operational technology (OT) from information technology (IT) networks; continuous monitoring that distinguishes cyberattacks from equipment failures; rapid incident response guided by pre-established protocols; and international co-operation through platforms like Information Sharing and Analysis Centres (ISACs), which enable collective defence.

Practical recommendations

- **Implement layered security architectures.** Adopt zero-trust principles throughout operational networks, implement strict network segmentation separating critical controls from business networks, and deploy continuous monitoring systems capable of distinguishing attacks from equipment failures.
- **Secure critical systems and distributed resources.** Deploy hardware-based security for critical control systems, implement encryption for operational data, and require multi-factor authentication. Mandate security standards for all grid-connected devices, require secure-by-design principles from manufacturers and rigorously protect aggregation platforms. Require regular cybersecurity awareness and skills training for staff.

- **Establish institutional frameworks for co-operation.** Define clear incident protocols with designated responsibilities, participate actively in threat intelligence networks such as ISACs, and co-ordinate with regulatory frameworks such as the European Union's Critical Entities Resilience Directive, Network and Information Systems Directive (NIS2) and Cyber Resilience Act.

Lesson 10: Build mechanisms for cross-border co-operation

High-impact events often exceed a single country's restoration capacity, requiring international co-operation for equipment, resources, expertise and knowledge-sharing. Shared resources and co-ordinated response capabilities are essential during rare but catastrophic events that can overwhelm national capacities. Effective mutual assistance requires frameworks to be established in advance rather than ad-hoc arrangements. Pre-existing agreements enable rapid deployment under established protocols, while their absence can delay recovery for months.

Ukraine's experience and lessons learned

International co-operation has proven essential to Ukraine's energy system resilience since 2022. The response included equipment donations through the Ukraine Energy Support Fund, international technical expertise, multilateral financial assistance and diplomatic support for cross-border electricity trade. Ukraine's strategic integration into the European Network of Transmission System Operators for Electricity (ENTSO-E) enabled import capacity to be increased twice: by 2 150 MW before winter 2025 and by a further 2 450 MW before winter 2026. As part of the response to the January 2026 attacks, Naftogaz and Ukrzaliznytsya were ordered to raise imports by up to 50% of their consumption to maximise utilisation of available capacities.

Equipment assistance scaled rapidly to meet critical needs. From 2022 through 2025, the European Union's Civil Protection Mechanism transferred 9 000 generators to Ukraine, with a further 2 500 generators delivered via a repurposed co-operation programme. Generator capacities ranged from 12.5 kVA to as much as 1 000 kVA, with the largest units capable of providing full electricity supply to hospitals during power outages. The United States also provided extensive assistance, including more than 3 600 generators. The transferred generators enabled critical repairs and secured uninterrupted electricity supply for smaller communities and critical facilities.

Several challenges emerged despite the scale of assistance, however. Equipment compatibility required significant engineering work to integrate donated systems.

Unclear prioritisation among donors complicated resource allocation. Logistical complexities arose when transporting large equipment across borders during active conflict. Co-ordination challenges multiplied across numerous parallel initiatives from different countries and organisations. The Ukraine Energy Support Fund, administered by the Energy Community Secretariat, proved to be an effective co-ordination mechanism.

Cross-border infrastructure vulnerability requires particular attention to resilience planning**.** This is particularly true for offshore infrastructure, which is often isolated and harder to access for repairs. A primary challenge for resilience assessment is evaluating the vulnerability of critical energy infrastructure to incidents like deliberate damage to undersea gas pipelines and power cables. An analysis of Baltic cross-border power disruption reveals potential technological and logistical bottlenecks that could cascade across regions (see Box: Cross-border infrastructure vulnerabilities in Europe).

International co-operation frameworks are expanding to include Ukraine. European countries are required to co-ordinate and agree on risk preparedness plans for electricity, as well as preventive and emergency plans for gas. Co-ordination groups for electricity and gas bring together EU Member states to share plans and align responses during crises. Moldova and Ukraine were invited to the solidarity test exercise performed jointly by the European Commission, the Member states, the European Network of Transmission System Operators for Gas (ENTSOG) and ENTSO-E in November 2024. This confirmed the important role of emergency plans in ensuring quick and efficient response to events affecting cross-border infrastructure and underlined the indispensable value of co-operation.

Practical recommendations

- **Leverage international forums to raise awareness, share lessons learned and facilitate co-operation beyond immediate neighbours**. Establish platforms for periodic exchanges that can be activated during emergencies.
- **Establish frameworks for mutual assistance.** Define clear obligations and cost-sharing arrangements through formal agreements. These should include regional co-ordination mechanisms, equipment-sharing protocols and technical co-operation frameworks that activate automatically during qualifying events.
- **Create regional strategic reserves and capabilities.** Maintain regional equipment reserves for critical spare parts and mobile generation capacity. Establish specialised registries of repair capability, identifying available expertise and equipment across countries. These should include priority access agreements to ensure rapid deployment.

- **Develop operational co-operation capabilities**. Conduct joint exercises regularly to test co-ordination mechanisms and identify gaps. Implement exchange programmes to build relationships among technical staff before emergencies occur. Maintain shared situational awareness platforms that provide real-time visibility of system conditions and available resources.
- **Address legal and financial barriers**. Establish legal frameworks enabling cross-border assistance, including liability protections, cost-recovery protocols, equipment customs exemptions and mutual recognition of professional qualifications.

Cross-border infrastructure vulnerabilities in Europe

Recent incidents across Europe reveal both the effectiveness of existing co-operation mechanisms and their limitations. Pre-existing agreements, like the Nordic co-operation, may enable rapid crew and timely equipment deployment during extreme weather events. Conversely, damage to the EstLink2 submarine cable in 2024 revealed that specialised repair ships were unavailable for months due to a lack of priority access agreements. This contrasts with the proactive approach taken by Réseau de Transport d'Électricité (RTE) of France and National Grid of the United Kingdom, who have negotiated priority access to repair vessels with shipping companies for North Sea cable maintenance.

Technical and logistical constraints significantly affect recovery timelines for cross-border infrastructure. Accordingly to the resilience assessment for power system disruptions of interconnectors in the EU region, repairing a single fault on a submarine high-voltage direct current (HVDC) cable typically takes two to three months due to inherent complexity: faults must be located precisely, repairs require specialised vessels, and operations depend on weather conditions and damage extent. Overhead high-voltage alternating current (HVAC) lines present different timelines: completely rebuilding a line can take five to six weeks, while restoring a single damaged transmission tower ranges from eight to 48 hours depending on damage severity.

Several factors compound recovery challenges. HVDC systems require complex fault diagnosis and repair. Specialised equipment – particularly submarine cable repair vessels – remains scarce globally. Modern cable systems' technical complexity further extends timelines. Most critically, simultaneous disruptions at multiple locations can dramatically increase repair times when multiple faults require the same specialised crews. International co-ordination for cross-border deployment of qualified technicians and shared access to specialised equipment can significantly accelerate repair efforts in such scenarios.

Acknowledgements, contributors and credits

This report was prepared by a team drawn from different parts of the International Energy Agency (IEA). It was designed and co-ordinated by Talya Vatman, Caspian and Black Sea Programme Manager, and Jacques Warichet, Analyst in the Electricity Systems and Markets Division. The lead authors were Ottavia Valentini, Talya Vatman and Jacques Warichet. Contributions were provided by Theresa Gebhardt (attacks on energy system), Markus Fager-Pintilä (data) and Ronan Graham (oil stocks).

Many ideas for this report came out of IEA missions to Ukraine, beginning in 2023, and through exchanges with Ukrainian and international stakeholders. Special thanks go to Pablo Hevia-Koch, former Head of the Renewable Integration and Secure Electricity Unit, for initiating the Ukraine power sector resilience workstream with Talya Vatman.

Valuable comments and feedback were provided by IEA senior management and other colleagues within the IEA, in particular by Mary Warlick, Keisuke Sadamori, Tim Gould, Dan Dorner, Ali Al-Saffar, Jason Elliott, Dennis Hesseling, Pablo Hevia-Koch, Erica Robin, Dan Wetzel, Hugh Hopewell, Christine Brandstatt, Theresa Gebhardt, Javier Jorquera and former analyst Craig Hart.

Nicola Clark edited the report. Thanks go to the IEA's Communications and Digital Office for their help in producing the report. Particular thanks go to Astrid Dumond, Liv Gaunt, Julia Horowitz, Irina Paun, Andrea Pronzati and Clara Vallois. Hyejeong Lee and Einar Einarsson provided essential support.

Many international experts provided input and reviewed a preliminary draft of the report. Their comments and suggestions were of great value. They include (in alphabetical order): Youssef Almulla (Danish Energy Agency), Olivier Arrivé (RTE and ENTSO-E), Petya Barzilska (European Initiative for Energy Security), Aliabbas Bhamani (National Energy System Operator), Olha Bondarenko (Helmholtz Centre Berlin), Ben Cooke (NATO energy security centre of excellence), Borys Dodonov (Kyiv School of Economics), Pernille Hagedorn-Rasmussen (Danish Energy Agency), Nazar Kholod (Pacific Northwest National Laboratory), Albéric Mongrenier (European Initiative for Energy Security), Helen Naser (GIZ), Susanne Nies (Helmholtz Centre Berlin), Olena Pavlenko (DiXi Group), Rouven Stubbe (Helmholtz Centre Berlin), Pat Tynan (National Energy System Operator), Jean-Francois Vuillaume (Joint Research Centre, European Commission), Katarina Yuen (Sweden's Energy Ministry) and Monika Zsigri (DG ENER, European Commission).

International Energy Agency (IEA)

This work reflects the views of the IEA Secretariat but does not necessarily reflect those of the IEA's individual Member countries or of any particular funder or collaborator. The work does not constitute professional advice on any specific issue or situation. The IEA makes no representation or warranty, express or implied, in respect of the work's contents (including its completeness or accuracy) and shall not be responsible for any use of, or reliance on, the work.

Unless otherwise indicated, all material presented in figures and tables is derived from IEA data and analysis.

IEA Publications
International Energy Agency
Website: www.iea.org
Contact information: www.iea.org/contact

Typeset in France by IEA - February 2026
Cover design: IEA
Photo credits: © Unsplash