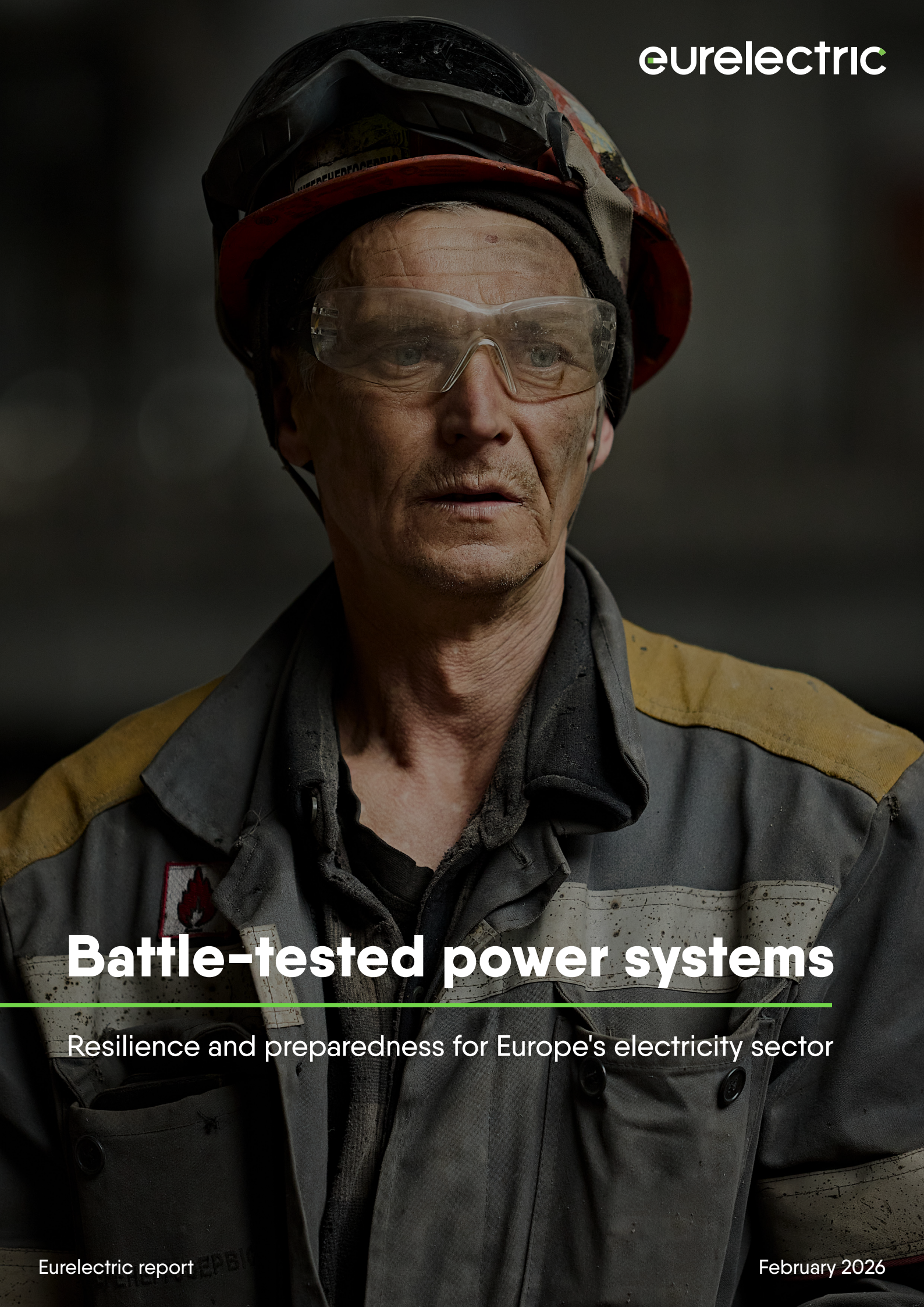


eurelectric

Battle-tested power systems

Resilience and preparedness for Europe's electricity sector

Eurelectric report

February 2026

Eurelectric represents the interests of the electricity industry in Europe. Our work covers all major issues affecting our sector. Our members represent the electricity industry in over 30 European countries.

We cover the entire industry from electricity generation and markets to distribution networks and customer issues. We also have affiliates active on several other continents and business associates from a wide variety of sectors with a direct interest in the electricity industry.

We stand for

The vision of the European power sector is to enable and sustain:
- A vibrant competitive European economy, reliably powered by clean, carbon-neutral energy
- A smart, energy efficient and truly sustainable society for all citizens of Europe

We are committed to lead a cost-effective energy transition by:

investing in clean power generation and transition-enabling solutions, to reduce emissions and actively pursue efforts to become carbon-neutral well before mid-century, taking into account different starting points and commercial availability of key transition technologies;

transforming the energy system to make it more responsive, resilient and efficient. This includes increased use of renewable energy, digitalisation, demand side response and reinforcement of grids so they can function as platforms and enablers for customers, cities and communities;

accelerating the energy transition in other economic sectors by offering competitive electricity as a transformation tool for transport, heating and industry;

embedding sustainability in all parts of our value chain and take measures to support the transformation of existing assets towards a zero carbon society;

innovating to discover the cutting-edge business models and develop the breakthrough technologies that are indispensable to allow our industry to lead this transition.

Dépôt légal: D/2026/12.105/02

Generation & Environment Committee
Energy Security Taskforce

Contact:
Lead author: Nic STEINWAND, Policy Advisor – EU Energy & Climate – nsteinwand@eurelectric.org
Contributing author: Silvia COSSA, Intern – Markets & Customers – scossa@eurelectric.org

Battle-tested power systems: Resilience and preparedness for Europe's electricity sector

A Eurelectric report February 2026

Executive summary

This report follows up on Eurelectric's study from February 2025, *Redefining energy security in the age of electricity*, to specifically address hybrid threats to physical electricity assets – one of the identified exogenous threats to Europe's energy security. To do so, the report delves into two dimensions:

1. **Deep dive on lessons learnt from Ukraine and recent events:** *Redefining energy security* included a case study on Ukrainian utility, DTEK, and their experience of the first three years of Russia's war of aggression. This report expands on this with a deep dive on Russia's tactics in Ukraine including the most recent events (to the end of 2025), the lessons learnt and assesses the hybrid warfare tactics being employed against EU Member States and lessons learnt from them as well.
2. **Benchmark European utilities preparedness for threats to physical assets:** while the EU is not in a hot war, hybrid warfare has become a new reality while geopolitical tensions continue to simmer. This report therefore benchmarks European utilities' level of preparedness for those threats and assesses how it stands up to the threat landscape.

Based on these findings, the report comes to three conclusions:

1. **Energy infrastructure is a target for adversaries and needs to be protected.** In a full-scale war scenario, energy assets are targeted by drones, missiles and shelling to knock out power and undermine society's morale and the efficacy of defence. Hybrid threats aim to do the same thing but with less predictability and attributability. Preparedness for and resilience to hybrid threats, is the minimum for us to do today, but we should be looking at the lessons from Ukraine to achieve a higher standard of protection which acts as an insurance policy in case of hybrid attacks and provides real mitigation dividends in case of war.
2. **Utilities are aware of the evolving threat landscape and are beginning to strengthen preparedness for today's increasingly complex threats.** A stark shift in the state of geopolitics has unfolded in just a few years that utilities are still adapting to. While there are variations based on threat exposure, utilities in Europe can take no regret steps towards improving readiness for emergency that limit exposure to various threats even beyond hybrid attacks.
3. **Utilities, Member States and the EU can take steps to improve preparedness.** Low-cost solutions to organisational preparedness exist such as increasing situational awareness, cooperating with local and national authorities and exercising crisis responses. At the same time, with the right economic incentives and supported by Member States, utilities can reinforce physical assets, stockpile critical equipment and increase cybersecurity efforts. On the policy side, the EU can take steps to accelerate implementation of key legislation at national level, as well as support critical infrastructure resilience through investment frameworks and defining a strong governance structure with guidance on how to identify threats in its revision of Europe's energy security architecture.

Battle-tested power systems: Resilience and preparedness for Europe's electricity system

01. Threats to physical assets: full-scale war and hybrid threats

Russia's war in Ukraine

Russia's illegal full-scale invasion of Ukraine that commenced on 24 February 2022 was a turning point for security in Europe – especially energy security. As of writing, Ukraine is still in a state of war with Russia targeting its critical energy infrastructure at an increasing pace and scale. Russia's strategy highlights a long-standing military doctrine dating back to the Soviet era where war plans targeted energy supply systems, including power plants.[1] As the war approaches its fourth year, the strategy remains central to Russia's war effort, and the Sisyphean challenge of powering Ukrainian society during that time provides important insights for the rest of Europe on best practices to protect electricity infrastructure from attack.

Russia's tactics in Ukraine

To date

While targeting energy infrastructure is one of the war's defining characteristics, the opening act of the war generally left it intact. Russia expected to take the capital, Kyiv, in three days and therefore left much of the infrastructure alone, as it would be needed once invasion gave way to occupation.[2] Of course, Kyiv did not fall. Ukraine mounted successful defence, pushing advances on the capital back and forcing Russia to refocus its efforts on the East to Southeast of the country.

The Armed Conflict Location & Event Data (ACLED) Ukraine Conflict Monitor tallied 1,065 attacks on Ukrainian energy infrastructure to the end of 2024.[3] The World Bank indicates this resulted in more than $20 billion (€17 billion) of damage to Ukraine's energy infrastructure.[4] It must be noted, however, that due to security considerations, exact numbers of attacks – and on which assets – are incomplete in public records, as making them public would aid Russia in its targeting campaign. This nonetheless implies that the data presented above are only the tip of a larger 'iceberg'.

Towards the end of 2025, attacks intensified. On 8 November 2025, a massive attack including 450 exploding bomber drones and 45 missiles targeted 25 locations across Ukraine, leading to power cuts in the Dnipropetrovsk, Chernihiv, Zaporizhzhia, Odesa and Kirovohrad regions.[5] In 2025 alone, a total of 1,225 attacks eclipsed the cumulative attacks of the prior three years.[6] The brunt of these attacks were made in the four final months of the year. Escalation of attacks began in September, ahead of winter; a particularly brutal tactic to subject the population to the cold and dark with disruptions in water supply and communications, sapping morale and endangering human life.[7] This is a centuries' old Russian strategy of dispatching 'General Winter' in its war efforts.

[1] International Institute for Strategic Studies (IISS), p. 4 (August 2025)
[2] Centre for Global Studies, p. 10 (July 2024)
[3] ACLED (retrieved on 22 December 2025)
[4] World Bank (February 2025)
[5] BBC, (8 November 2025), retrieved on 13 November 2025
[6] ACLED (retrieved on 9 January 2026)
[7] ACLED (retrieved on 14 November 2025)

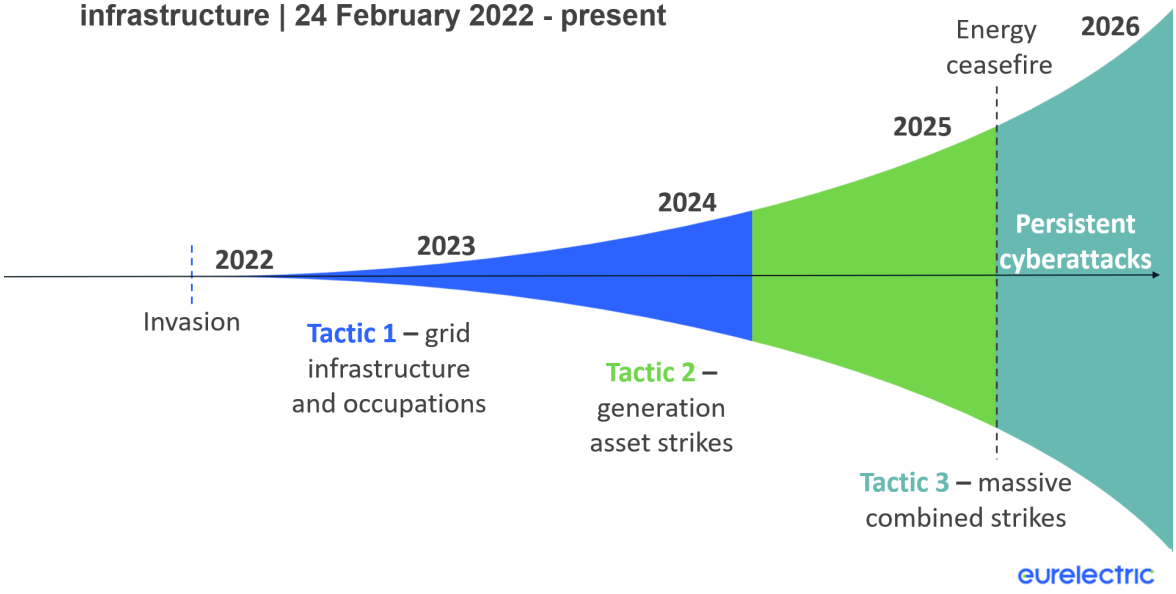
Evolving tactics

As the war continues to progress, Russia's tactics have evolved, utilising new battlefield technologies and targeting tactics to destroy Ukrainian energy infrastructure. Rasmussen Global identifies three attack categories including missile attacks, drone and artillery strikes and armed forces occupation.

From the beginning of the war to today, the more conventional tactic of shelling by artillery has increasingly given way to drone and missile warfare. Iranian-made Shahed unmanned combat aerial vehicles (UCAVs) have been infamously used for kamikaze-style attacks. Missile strikes have also increasingly become more precise, improving targeting enough to execute 'double-tap strikes' whereby drones are launched *en masse* as a first strike to create holes in reinforced protections, enabling precision missile strikes to destroy equipment behind said physical protection. Occupation is also a ubiquitous risk in all full-scale war. However, given limited advances since the initial phases of the war, this tactic has been less exploited than the former two.[8]

In *Redefining energy security*, distinct waves of attack were identified based on the assets targeted.[9] Since the publication of that report, attacks in 2025 intensified despite the *de facto* limited ceasefire on energy infrastructure agreed between American President, Donald Trump, and Russian President, Vladimir Putin, on 23 March.[10] Meanwhile, throughout the war, cyberattacks have also been an instrumental Russian tactic that cannot be overlooked. Figure 1 shows the increasing scope of attacks throughout the war from 24 February 2022 to present.

Figure 1: Increasing scope of Russian attacks on Ukraine's energy infrastructure | 24 February 2022 - present



Tactic 1 - grid infrastructure and occupations

At the beginning of the full-scale invasion, grids were disconnected as Russian troops advanced and energy infrastructure was caught in the crossfire. The invasion date non-fortuitously coincided with a scheduled three-day disconnection of the Ukrainian grid from the Russian and continental

[8] Rasmussen Global, pgs. 4-5 (3 June 2025)
[9] Eurelectric, pgs. 64-65 (13 February 2025)
[10] Security Council Report (25 March 2025) retrieved on 30 November 2025

European grids, as the country ran tests in island mode in preparation for connection with the European power system (which was eventually accomplished in March 2022). This timing highlights Russia's awareness of and willingness to exploit energy's role in broader security efforts, using it to hamper military and defence capabilities.[11]

Shortly following the invasion, Russia began unprecedented shelling of the Zaporizhzhia nuclear power plant (NPP) on 2 March 2022, despite such an act's explicit prohibition in Additional Protocol II to the Geneva Conventions, Article 15.[12] Following this, as the Russian army advanced, they occupied the Zaporizhzhia NPP, several thermal power plants (TPPs), wind and solar farms. It was not until 11 September 2022 that they began their sustained campaign of targeting electricity infrastructure.

Then, in autumn of 2022, targeted shelling of transmission system substations split Ukraine into three energy islands, cutting supply to two-thirds of all consumers.[13] Russia's objective became the fragmentation of the United Energy System (UES) by severing the link from the Right Bank (West) of the Dnipro River to the Left Bank (East), where Russia had shifted its military focus.[14] This strategy remains central. However, Ukraine's effective response managed to reconnect the system (and keep it connected), which led to a new tactic.

Tactic 2 – generation asset strikes

Once Russia realised Ukraine's ability to successfully respond to attacks on transmission infrastructure and undermine their initial objective, focus shifted to generation assets. These included TPPs and hydroelectric dams, as well as substations for NPPs – large, centralised targets with high capacity that continue to provide large shares of Ukraine's electricity mix and system stability. Russia's objective was to collapse centralised electricity and heat supply for Ukrainians via combined missile and drone attacks.[15] More strategically, the objective was to create over- and under-energised parts of the grid along the West-East Dnipro divide.

The tactic proved extremely effective. The Centre for Global Studies summarises that as of September 2023, Russian troops fired more than 6,500 missiles and 3,500 drones over Ukraine, destroying about 50% of Ukraine's energy infrastructure and decreasing electricity generation capacity by about 50% compared to pre-invasion with more than 67% of thermal generation capacity lost. This led to serious challenges to balance the UES[16] and served as a wake-up call for Ukraine's European allies. In response, an agreement with ENTSO-E in October 2024 increased cross-border capacity between the EU and Ukraine from 1.7 GW to 2.1 GW,[17] and 2.5 GW in emergency situations.[18] However, this cross-border capacity generally serves the over-energised portion of the grid in the West and does little to support the grid in the East.

A further evolution of Russian tactics came when they began targeting wind and solar substations. This was made possible due to expanded munitions production capacity as the country transitioned more fully into a war-time economy. This was, however, a less successful tactic. Rasmussen Global found that wind turbines were targeted more than solar panels, since they consist of large

[11] Center for Security Studies (CSS), ETH Zürich, pgs. 10-11 (March 2025)
[12] United Nations, p. 320 (1977)
[13] Ośrodek Studiów Wschodnich (OSW), (18 January 2023) retrieved on 14 November 2025
[14] Centre for Global Studies, p. 26 (July 2024)
[15] *Ivi,* p. 21
[16] *Ivi,* p. 33
[17] ENTSO-E (29 October 2024)
[18] Eurelectric, p. 64 (13 February 2025)

components that are expensive to replace with long production lead times and more complex repairs, as they must be conducted at height and require cranes. Due to the distributed nature of RES as well, there is a cost calculation – a morbid 'bang-for-buck' consideration of the opportunity cost of using a missile that costs millions of euros to target a few megawatts of RES versus the high hundreds of megawatts of more centralised capacity. For this reason, most RES targeting involves the collection points like nodal substations that injects larger quantities of RES generation to the wider grid, rather than the generation assets themselves.[19]

Tactic 3 – massive, combined strikes

Since September 2025, some of the most intense attacks of the war have taken place. Russia has launched over 200 attacks on TPPs alone, particularly in the east of the country.[20] In October 2025, the United Nations' Office of the High Commissioner for Human Rights decried three large-scale combined strikes that month targeting energy infrastructure, highlighting "significant risk of dangerous consequences for civilians this winter, including prolonged disruptions to heating [and] electricity".[21]

DTEK, Ukraine's largest private utility, recounted to Eurelectric in the drafting of this report that, while the ceasefire was instrumental in giving it time to bring destroyed capacity back online, the latest Russian tactics have been brutal. Drone production capacity has reached critical mass, and attacks now see hundreds of drones target specific critical targets in a first onslaught, followed by three to five precision missiles to deal a *coup de grâce*, overwhelming even the strongest fortifications. The sheer number of munitions used means even with a 60-70% shoot-down rate, the few that get through remain fatal. This applies both to infrastructure and to the human crews on site. As waves pass, people spring to action only to be caught in the next onslaught. It is worth noting the commendable efforts of these people on the ground. In the final weeks of 2025, Russia has continued to scale up attacks on substations causing massive outages, but thanks to repair crews' efforts, swift reconnection of hundreds of thousands has continued to be possible.

At the time of writing, Ukraine is fighting through its fourth winter of the war; it will be the toughest yet. Increasingly, gas has become a target as well since gas transit through Ukraine ended at the beginning of the year.[22] Meanwhile, the strategy remains to split Ukraine into numerous energy islands, disconnected from each other. The two most targeted pieces of equipment are, on the gas side, compressors, and on the electricity side, primary transformers, due to their vital role in the system, long lead times and difficulty to repair. Massive, combined strikes on these chokepoints in the system are expected to continue at pace and scale – like the combined strike on 27 December 2025 that prompted DTEK into swift action to reconnect over 1 million customers in the Kyiv region[23] – to cripple Ukraine's energy system and undermine the country's morale and ability to defend itself from the invader.

Persistent tactic: cyberattacks

Part and parcel of Russia's physical attacks on energy infrastructure are the accompanying cyberattacks. Cyberattacks have been a constant in Ukraine – pervasive throughout all waves of physical attacks and having increased by 30-40% since the invasion began, according to DTEK.

[19] Rasmussen Global, p. 8 (3 June 2025)
[20] DTEK (23 December 2025) retrieved on 24 December 2025
[21] United Nations Office of the High Commissioner for Human Rights (OHCHR), (30 October 2025) retrieved on 14 November 2025
[22] European Commission (31 December 2024)
[23] Reuters (28 December 2025) retrieved on 12 January 2026

Artificial intelligence (AI) has also advanced tremendously since the beginning of the invasion, leading to an arms race of increasingly sophisticated models attacking one another. Russia might apply a new AI model to hack Ukrainian systems, but Ukraine deploys models to counter and block them. Instead of human hackers fighting back and forth for months, this task can now be automated by AI.

Given the clandestine nature of cyber activity, however, the exact tactics are less well documented. In *Redefining energy security,* it was noted that in the build-up to the full-scale invasion, cyberattacks were employed as a hybrid tactic. A baseline level of cyber activity generally exists, but just before the invasion, the scale and scope of cyberattacks increased significantly. Millions of attempted infiltrations signalled a grander strategy supported by a foreign State adversary to take critical energy infrastructure offline and sow confusion.[24] This remains part of Russia's strategy, alongside disinformation campaigns. Widespread campaigns claimed falsely, for example, that rolling blackouts were a consequence of electricity exports to Europe rather than the destruction of infrastructure.[25]

One large-scale attempted attack involves the Russian military intelligence (GRU) unit known as Sandworm. In April 2022, they attempted to deploy Industroyer2 malware, among others, against high-voltage substations to cause widespread power outages. Operatives were able to move from its target's information technology (IT) network to its industrial control system (ICS) network, but CERT-UA, working with the Slovakian internet security company, ESET, were able to stop the attack before it spread.[26]

Lessons learnt from Ukraine

Across the four waves of physical attacks and pervasive cyberattacks and disinformation, myriad lessons can be taken on what measures support the resilience of a power system under fire. While in a war-time scenario, the first line of defence is the military, the power companies themselves are also on the front line and need to be protected accordingly, as electricity is necessary for a functioning modern society as well as military operations and, in Ukraine's case, was quickly caught in the crossfire.

The military is naturally responsible for the defence of assets, whether by defending a position to avoid occupation or deploying ground and air defence to shoot down incoming drones and missiles. This is outside the operational scope and capabilities of power companies (to say nothing of the legality of the use of force by a civilian organisation and that assigning them responsibility for the impacts of hostile attacks would imply unmanageable legal responsibility). The onus nonetheless falls on power companies to practice effective preparedness, centring around three phases from pre- to post-event that that this report focuses on – preparation, response and recovery. What should be noted, however, is that there is not a one-size fits all solution, and different assets will also require tailored approaches to ensure their resilience.

1. Preparation

The crucial first step to preparedness is the preparation, which for power companies includes anticipating threats to assets and taking steps to prevent damage, wherever possible.

Based on the experience in Ukraine, there are several effective measures to be taken:

[24] Eurelectric, p. 64 (13 February 2025)
[25] Center for Security Studies (CSS), ETH Zürich, p. 17 (March 2025)
[26] Canadian Centre for Cyber Security, pgs. 2-3 (22 June 2022)

- **Situational awareness and collaboration:** before knowing what to prepare for, power companies need a keen understanding of the threats they face. Generally, the military and clandestine services of a country have a monopoly on this information, but to prepare effectively, power companies need to be briefed in on the threats they are expected to respond to. This makes the case for greater, more formalised collaboration between these services and the power companies. Ensuring a minimum level of situational awareness helps the power companies understand the threat landscape, but it also helps them provide better information to security services, making the collaboration a two-way street of information that is useful for both parties. This concretely means that a crisis intervention team within a given energy company needs to be trusted with classified information, as they will only be able to prepare and eventually react if they properly understand risks, threats and countermeasures in (hybrid) warfare.
- **Hardening assets:** physical fortifications around critical energy infrastructure can include gabions, sandbags, concrete blocks and specialised nets to defend against drones. This is the most common form of hardening and practiced by most companies in Ukraine due to its cheap and quick deployment. More advanced measures are, however, also possible such as infrastructure built by design with fortification in mind.[27] EU countries closer to the border with Russia are acting on this, investing in drone barriers, concrete shielding for substations and buried assets.[28] However, due to cost, it can be more prudent in a war-time scenario to focus on protection of the most critical links in the system – for example, nodal substations for a wind farm, rather than individual turbines. These decisions must be coordinated with Member States, since the scale and nature of the required protections can go beyond companies' responsibilities.
- **Cybersecurity:** a robust cyber-protection system for dispatching centres, UES regional control centres, key substations and generation facilities helped Ukraine's energy sector withstand massive Russian cyberattacks before and in the first days after the invasion.[29] At the same time, supportive systems such as enterprise risk management (ERM) systems and internal communications are sources of potential critical information for an attacker to gain vital understanding of the effectiveness of its attacks and therefore should be strongly protected as a matter of strategic importance. Meanwhile, mis- and disinformation can undermine credibility and effectiveness of response which can be countered by proactive communication with the public.[30]
- **Mental resilience:** in war time, workforce rapidly evaporates as personnel either tend to prioritise personal and familial needs first or flee the country, join/are drafted into the military or are unfortunate casualties of the struggle. For those who are left, there is more work to do and under much more stressful conditions. Following long-term exposure to threats, individuals also risk adapting to the *status quo*. It is vital for personnel's safety, however, to remain vigilant and aware of the continued risks.[31] It is therefore vital to prepare personnel's mental resilience by normalising discussions about preparedness, educating them on safety measures in place and providing training and retention guarantees for the response.

[27] Rasmussen Global, pgs. 4-5 (3 June 2025)
[28] The Economist (16 October 2025)
[29] Centre for Global Studies, p. 7 (July 2024)
[30] Rasmussen Global, p. 6 (3 June 2025)
[31] *Ivi,* pgs. 7-15

- **Training:** includes drills with staff, exercises with local authorities. Anti-crisis response teams may be set up to respond pre-emptively and in case of crisis ensure a line of communication with public authorities and the military. Emergency protocols should also be in place to ensure response is premeditated, practiced and effective as well as ensure that staff are aware of the safety provisions in place such as bunkers and communication channels. Finally, training should be ongoing to prevent complacency and pre-emptively support mental resilience.
- **Stockpiles:** lead times for critical equipment can already be long in times of peace. In times for war, supply chains are subject to far more disruption. Equipment availability dries up quickly as repairs to damaged equipment increase in response to attacks. While stockpiles of equipment can help mitigate this impact, companies need to be prepared for attrition and the costs for having all equipment stockpiled would be untenable. Having the most critical equipment in stockpile such as transformers is therefore the most effective approach, and stockpile locations should be kept secret, decentralised and/or protected from attack. Outside of a war-time scenario, stockpiling efforts and levels needed can vary significantly depending on the threat scenarios, as the requirements for addressing routine disruptions are very different from those for coping with large-scale, high-intensity events and should be agreed between companies and national authorities. Meanwhile, solutions like the 'Mobile Brigade' – pioneered by Ukraine's energy ministry to identify and collect equipment from decommissioned assets across Europe – help procure replacement equipment, while the cannibalisation of destroyed assets that cannot or should not be repaired can also fill equipment supply gaps.[32,33] Finally, we should also consider the workforce and the repair skills they bring as a scarce resource that needs to be stockpiled and managed - ready to respond as the crisis develops.

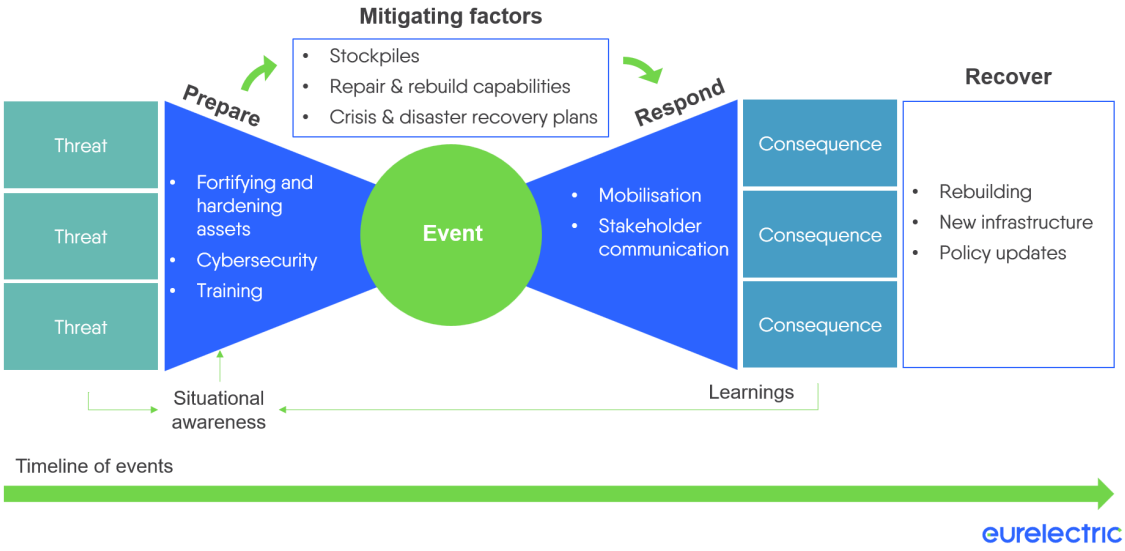
2. Response

Not every attack can be avoided. In a war-time scenario, damage and destruction is inevitable. We can think of it like a bowtie – with two ends that get increasingly broad, representing the actions taken to prepare, and the actions taken in response. The preparation taken in the section prior supports the response by providing mitigating factors. If those are strong and precise, they can reduce the impact of the event represented by the size of the knot in the middle (see figure 2).

Following the event, the response is the immediate reaction to a crisis which requires personnel to be mobilised, initiate emergency procedures, get to and repair damaged assets. If possible, the response should also ensure restoring power and cooperating with the military to ensure safety as well as support the military's situational awareness all in an efficient and effective manner.

[32] Rassmussen Global, pgs. 7-15 (3 June 2025)
[33] Eurelectric, p. 65 (13 February 2025)

Figure 2: Bowtie model for preparedness



A crisis (or anti-crisis) response team should be in contact with the energy ministry and military to report damages. Rapid repair crews may need to be dispatched to address the damage if it is feasible. In Ukraine's experience, if not repairable, assets may nonetheless be cannibalised with remaining working equipment recovered and used at other assets, less exposed to attack.[34] This was DTEK's approach once it saw that one of its assets was likely to be captured by enemy forces. The company disassembled an entire TPP in the months before the final attack. This equipment is now retrofitted into other plants when they are hit or are stockpiled for the likely event of another attack. Experience in Ukraine has also demonstrated that it can sometimes be more pragmatic to repair equipment, rather than prevent damage with expensive asset fortifications, making efficient and effective response crucial.[35]

The military must also be included in the response. Following an attack, the military is the first on site, as they must clear the facility, identify and neutralise life-threatening damage, and only afterwards permit civilian personnel to re-enter the facility. This is also the case in post-occupation, as sites require military inspections for mine clearance and removal of other threats.[36]

3. Recovery

The final step, recovery, coming after the initial response, may be delayed in case of war. A state of normalcy in ongoing conflict will remain elusive and further attacks can occur. While the restoration of power is an immediate step towards recovery, solutions may be *ad hoc* and insufficient in the longer term. Manpower and access to equipment and construction material, as well as proximity to the frontline will impact decisions on how to proceed, and backups to backups may be necessary if assets are retargeted. As mentioned above, it may be more pragmatic to cannibalise an asset than to repair it.[37]

In the longer-term, efforts to restore the system to pre-war levels will need to be taken. New assets will need to be built, and this provides the opportunity to build more secure assets. The case of Ukraine has demonstrated the vulnerabilities in centralised assets with large capacities, due to their

[34] Eurelectric, p. 65 (13 February 2025)
[35] Rasmussen Global, p. 8 (3 June 2025)
[36] *Ivi,* p. 11
[37] *Ivi,* p. 14

vital role in system stability. As a result, to increase energy security, investment decisions are steering towards increasing decentralisation through distributed RES such as wind and solar while balancing the need for more flexibility and system stability in the system that can be provided by conventional assets like (pumped, especially) hydropower and nuclear (especially small modular reactors), as well as emerging technologies like battery energy storage systems (BESS) and demand-side flexibility.[38] This more decentralised and complex system also means there is a need for more advanced observability and steering technologies to run the system successfully, especially under concrete threats and enemy fire.

Understanding that the threat from Russia is likely to persist for years to come, Ukraine has identified increased decentralisation of its energy system as a matter of national security and its national energy and climate plan (NECP) has a target for a 27% share of distributed energy resources (DERs) in energy consumption for 2030.[39] DTEK is getting on and building these decentralised assets, having completed phase one of its Tyigulska wind farm during the war and has already started construction of phase two - creating 500 MW of capacity. In September 2025, it opened 200 MW of BESS, using batteries from Fluence. The project is spread across six sites in central Ukraine to minimise the effectiveness of any Russian attack.[40] Meanwhile, considerable room still exists for centralised assets, which, based on lessons learnt throughout the war, will need to be built harder and more resilient to withstand attacks, with standardised parts and equipment that can be rapidly replaced when needed.

While the EU is not involved in a hot war today, these lessons are important. Ukraine was already invaded by Russia in 2014 and understood their hostile intentions, but the scale of energy infrastructure targeting prompted scrambled action as this campaign ensued.[41] In the EU, we cannot afford to wait and see. German political and military planning is based on a Russia capable of invading NATO allies in Europe as early as 2028[42] and hybrid threats are already having real impacts on energy infrastructure in the EU. The lessons learnt in Ukraine provide actionable ways for us to mitigate these impacts, respond when they happen and recover in the aftermath, while also preparing us in case of the worst. The following section looks at this more in depth.

Hybrid threats in the EU

The new geopolitical reality merging out of Russia's unprovoked act of aggression echoes the proxy wars of the Cold War, but with a more active and dangerous component for non-combatants. A state of hybrid warfare also exists where so-called 'grey zone' physical and cyber tactics are being used by the Russian Federation and its loose network of operatives to give plausible deniability to outright attempts at undermining the EU's security. This includes our energy security.

Because these threats take place in a 'grey zone', it is often difficult to identify and attribute the actor behind the attack. Sometimes, it is possible to do so, but still with a level of plausible deniability of intent and/or connection to the actor in question. It is for this reason that Russia cannot be considered the only hybrid actor in this space. Nonetheless, we can identify that Russia is waging a shadow war on the EU, and the North Atlantic Treaty Organization (NATO) by extension, to destabilise, distress and deter support of Ukrainian sovereignty. These are calculated efforts to undermine democratic values, sow distrust within our society and destabilise common efforts.[43]

[38] Eurelectric, pgs. 65-66 (13 February 2025)
[39] Foreign Policy Analytics (November 2025)
[40] DTEK, retrieved on 17 November 2025
[41] Rasmussen Global, p. 7 (3 June 2025)
[42] euronews (3 December 2025) retrieved on 19 December 2025
[43] Commission on Security and Cooperation in Ukraine, pgs. 2 & 4 (2024)

The strategy is effective because it operates below the threshold for triggering a decisive, unified EU response. The inch-by-inch approach of escalation enables progressively more belligerent actions, where no clear line by any single action is crossed and the political will to respond to all prior actions as a cumulative line crossed is low. As a result, we are yet to see harsh consequences and hybrid threats keep coming. This ultimately underlines a strategy capable of causing panic and decreasing public trust. A first recommendation is therefore to "keep calm and carry on", or as Finnish President, Alexander Stubb, puts it, remain "calm, cool and collected" so we can focus on addressing the problem[44] – preparedness will help us get there and by doing so, undermine the objective of the ongoing hybrid assault.

Hybrid tactics

This section focuses on the grey zone tactics used to cause physical damage to energy infrastructure as well as malicious cyber activity being deployed to disrupt it. However, the strategy goes beyond simply taking power offline, and the European Commission has identified it as a permanent feature of today's reality in its communication on the European Union Preparedness Strategy.[45]

Hybrid threats short of full-scale war preclude any direct targeting of assets by Shahed drones, missiles or artillery by the Russian military – this would be considered an act of war. Still, there are ways to cause physical damage that remain below the threshold for war. Already, subsea cables have been damaged by vessels dragging their anchors. At the same time, utilities also face increasing levels of cyber threats, giving attackers the potential to control electricity system equipment connected to the internet, which would enable them to cause physical damage through dysregulation and subsequently, blackouts. More recently too, drones and airspace violations are raising concern of further means of hybrid attacks that are blurring the line between war and peace. Concerns are also mounting around technology supply chains and potential hidden 'kill switches' or 'bugged' equipment (particularly, solar inverters), which need to be considered when procuring system inputs from potential adversaries.

To date

Adversaries are actively testing Europe's resolve. Dragonfly Intelligence has mapped the intensity of the threat for EU Member States and shown a link between the amount of hybrid influencing experienced and overall level of support for Ukraine. Over the ten-year period from 2014 to the end of 2024, they attributed 219 acts of hybrid warfare in Europe, of which 86% have taken place since Russia's invasion of Ukraine with 45% taking place in 2024 alone. 11 of these attacks targeted critical infrastructure.[46]

Regardless of who the actor is, hybrid events are happening at increasing scale and scope, which comes at a cost for utilities to repair and maintain operational continuity. The high-profile sabotage of Nord Stream 1 and 2 on 26 September 2022 kickstarted the hybrid tactics used against EU critical energy infrastructure and the pipelines have not been restored to operation since. Figure 3 highlights the full span of hybrid attacks from 24 February 2022 to present.

[44] eunews (11 April 2024) retrieved on 9 January 2026
[45] European Commission, p. 1 (26 March 2025)
[46] Dragonfly Intelligence, p. 8 (February 2025)

Figure 3: Timeline of hybrid activity 24 February 2022 - present

Subsea cables

The Baltic Sea is a hotspot for sabotage incidents. On 25 December 2024, Cook Islands-flagged Eagle S dragged its anchor and cut the Estlink-2 undersea cable in the Gulf of Finland. Before that, on 17 and 18 November, Chinese flagged Yi Peng 3 is suspected of having deliberately dragged its anchor to cut the C-Lion1 cable connecting Finland and Germany and Arelion cable linking Sweden and Lithuania. In the European Commission's energy security fitness check, it is said that Estonian authorities identified that the 25 December outage of EstLink-2 alone cost between €50-60 million in repairs alone.[47] The International Institute for Strategic Studies' calculates that a severed cable or pipeline costs tens of millions of euros, not including the economic damage from lost capacity or the additional costs of policing, investigating and defending the maritime domain.[48] For example, in direct response, NATO launched the Baltic Sentry mission in January 2025 to better protect and deter attacks on critical assets in the Baltic Sea. However, NATO's former Assistant Secretary-General for Innovation, Hybrid and Cyber, Jean-Charles Ellerman-Kingombe, quickly recognised the costly nature of the mission, resulting in a shift from 'robust military presence' to unmanned vehicles patrolling the Sea, reducing the deterrence factor against further attacks.[49]

Cyberattacks

Cyberattacks are also lucrative grey zone tactics employed increasingly, since the domain is digital and relatively anonymous. Dragonfly Intelligence has also tallied 23 successful cyberattacks on Europe's energy sector from the start of the war in Ukraine to 8 October 2024.[50] On day one of the war in Ukraine, a suspected Russian cyberattack disabled remote monitoring via satellite for 5,800 German wind turbines, accounting for 11 GW of capacity.[51] The largest cyberattack to date has been the coordinated attack on 22 Danish energy companies in May 2023 led by Russian GRU group

[47] European Commission, p. 57 (22 December 2025)
[48] International Institute for Security Studies, p. 10 (August 2025)
[49] *Ivi,* p. 11-12
[50] Dragonfly Intelligence (18 October 2024), retrieved on 18 November 2025
[51] pv magazine (1 March 2022), retrieved on 19 November 2025

Sandworm. Sandworm operatives exploited zero-day vulnerabilities in Zyxel firewalls, forcing the affected companies to go into island mode to mitigate the spread.[52] More recently, an attack against Polish energy infrastructure gave hackers access to combined heat and power plants and RES generation management systems on 29 and 30 December 2025 which was successfully defended against, avoiding blackout or other negative consequences.[53]

A further example emanating from Russia was an attack on the Lake Risevatnet dam in Norway in April 2025. Hackers managed to open the water valve to full capacity enabled by a weak ICS password, draining water in the reservoir.[54] While not a hydroelectric dam, the incident demonstrates that malicious cyber activity can have physical consequences for assets. It also highlights a successful hybrid operation – the real impact was relatively benign, but the psychological impact is immense as it helps push a narrative that adversaries can gain control over our critical systems when they want, despite the reality of it being a small and particularly under protected system. The public thinking turns to the consideration that, had it been larger scale, it could have been a public safety crisis leading to flooding and potential loss of life. Had it been a hydroelectric dam, the drained water would have represented lost potential energy for the electricity system, impacting security of energy supply. Overall, the uncertainty such actions sow is an arguably more valuable outcome than any real damage caused.

Aerial threats

Numerous sightings of unidentifiable drones have been made in EU territory, representing a further potential threat.[55] The drones are very different than the Shahed drones used by Russia in Ukraine, more akin to commercial off-the-shelf-drones (COTS). Still, Ukraine has made extensive use of COTS drones to lethal effect on the battlefield,[56] meaning an adversary could also decide to repurpose a COTS drone to wage a hybrid war in the EU. Should Russia decide to, it could easily equip one (or many) of these drones with an explosive device to damage critical points in the electricity system, expanding physical hybrid attacks to beyond the maritime domain.

Beyond this, Russia has also blatantly disregarded EU airspace in Poland, Romania and Estonia. In Poland, on 10 September 2025, 21 Russian drones breached national airspace in the largest airspace breach since the beginning of Russia's invasion of Ukraine. At least three drones were shot down.[57] In Romania, on 13 September 2025, during a Russian attack on Ukrainian infrastructure, a drone breached the country's airspace. F-16 fighter jets were scrambled, coming close to taking down the drone before it left national airspace toward Ukraine.[58] In Estonia, the most egregious example took place on 19 September 2025 when three MiG-31 fighter jets flew into the country's airspace over the Gulf of Finland for 12 minutes before being escorted back to international airspace by two Italian NATO pilots in F-35 fighter jets.[59] While none of these airspace breaches represented a direct attack on critical infrastructure, they easily could have caused damage. This demonstrates the very thin line between a hybrid conflict and an outright state of war, and why preparedness for wartime broadly overlaps with the preparedness needed in the EU today.

[52] Sarah Braithwaite, *University of Hawai'i-West O'Ahu* (8 December 2023), retrieved on 18 November 2025
[53] Kancelaria Prezesa Rady Ministrów (15 January 2026)
[54] Kapersky ICS CERT (9 October 2025), retrieved on 18 November 2025
[55] The Observer (17 November 2025), retrieved on 18 November 2025
[56] Farrell Gregory, Emerging Threats Working Group (4 March 2025), retrieved on 18 November 2025
[57] Arms Control Association (October 2025), retrieved on 18 November 2025
[58] Reuters (13 September 2025), retrieved on 18 November 2025
[59] Security Council Report (21 September 2025), retrieved on 18 November 2025

Lessons learnt from hybrid threats

Both physical and hybrid tactics present clear challenges. Physical attacks can cause serious, expensive damage and sever energy systems leading to economic losses and strike fear in the public. Cyberattacks can do the same from afar as can the aerial threats posed by drones. Beyond this, there are myriad other hybrid threats that can impact the energy system. Power companies should also keep on the lookout for:

- Equipment theft (economic and security threat)
- Corruption like undermining protocols and safety codes (internal threat)
- Bomb threats (psychological threat)
- Arson attacks (physical threat)
- Hostage taking and terrorism including attacks on personnel (safety and physical threat)
- Industrial espionage like stealing sensitive security and operations data (internal threat)
- Supply chain infiltration like equipment bugging or kill switches (economic and security threat)
- Dis- and misinformation (psychological threat)

Like the military's role in wartime, deterrence is the frontline against such hybrid tactics. Eliminating the adversaries' plausible deniability and promising swift, united response with harsh consequences (potentially even military response such as shooting down drones or commandeering rogue vessels) for the adversary drives up the perceived cost and dissuades the adversary from initiating them. Short of that, these tactics will be used. Up until now, the EU has been unable to make deterrence credible, with governments frequently taking defensive, reactive measures and focusing on protection rather than the assertive steps needed for real deterrence.[60] This is part and parcel of preparedness and should not be overlooked at a political level.

Against this backdrop, power companies need to practice effective preparedness with Member State support. Preparing for, responding to and recovering from hybrid attacks is a new normal that this report argues should be a key element of Member States' priorities and power companies' strategy going forward. We see varying levels needed based on proximity to the frontlines with Russia, but it is also important to consider that the threat of these tactics increases based on the State's support for Ukraine, as mentioned above.

Preparation

Much like the wartime scenario, many of the same preparations hold. Hardened assets, cybersecurity, training and stockpiles are all important strategies to implement ahead of a hybrid attack – when it arrives, it is too late. Countries closer to the front are already moving to fortify critical infrastructure, as indicated above. Cybersecurity is as valuable in wartime as it is in peacetime, since the attacks faced are similar and require the same level of preparedness. Training ensures personnel are ready to respond to these low frequency, high impact events while stockpiles help avoid long lead times for critical equipment needed for a rapid response. At the same time, ensuring there are backup solutions for communication ahead of time ensures that essential stakeholders can share essential information.

What changes in this case is that the decision to prepare is not inspired by absolute necessity, but by will. A key part of preparation, therefore, is awareness of the threat landscape that provides motivation to address it. This report aims to raise that awareness, but another way to achieve it is

[60] International Institute for Security Studies, p. 4 (August 2025)

pre-emptively increasing cooperation and information sharing with authorities. Meanwhile, funds are on the table to address the costs involved. NATO-allied countries agreed to raise defence spending to 5% of gross domestic product (GDP) with 1.5% earmarked for defence-related investments, including cybersecurity, critical infrastructure protection and crisis preparedness. Eurelectric advocates for power companies to be able to tap into this pot of around €250 billion for preparations.[61]

Response

In the case of hybrid threats, what is important is rapid response – especially if the result is a massive power outage. Societal function degrades the longer it is without power, and effective and efficient response is critical for public safety. Differing from the wartime scenario, though, is that the risk to personnel is lower during recovery than the wartime scenario. Well-trained recovery teams with the right equipment available and potential off-the-shelf response plans can respond to an attack rapidly without putting their life on the line or having to consider the opportunity cost of asset cannibalisation. Therefore, key success factors include the resources and capabilities to repair, reinforcing the importance of training and proportionate stockpiling of critical equipment in the preparation phase.

Since other power companies will also not be subject to attrition of stockpiles and may not need to respond to a crisis themselves, strategic partnerships can provide provisions to support one another, alleviating the pressure on individual companies for the capabilities needed, whether it is expertise, equipment or manpower. What remains crucial is also the need to proactively communicate with local authorities and the public – especially customers that may be facing power outages – to maintain trust and aid in faster recovery time.

Recovery

Going forward from a hybrid attack, recovery constitutes acting on the lessons learnt from the experience. It can be argued that this section of the report is, itself, a recovery action, advocating for action based on the hybrid threats we have so far experienced. But beyond that, recovery ought to focus on increasing the cost of attack to deter it in the future. For example, offshore wind parks in the North Sea have already become the subject of the Russian navy's interest according to neighbouring countries,[62] and this is certainly because no major repercussions came from actions in the Baltic Sea. Hackers, too, have yet to face a court date or even be identified for their violations. Aside from the three drones shot down in Poland, no order exists to shoot down suspicious drones over critical infrastructure.

Lacking this deterrence, the next option in line is hardening assets as we rebuild and repair, making them more resistant to aggression based on the attack medium used. As established above in the case of Ukraine, more decentralised assets are generally more able to withstand attacks, and flexibility solutions provide security of supply, making longer term recovery one in the same with the continuation of the ongoing energy transition. Meanwhile, for cyberattacks, hardening might include simply implementing stronger security protocols. Critical assets should be protected with robust passwords and potentially authentication at a minimum. The recovery effort might therefore overhaul the passwords used for energy systems impacted, and more deeply take a cybersecurity by design approach that recognises the digital operation environment as one in the same with a modern power system's security. As for aerial threats, despite not suffering damage

[61] Eurelectric, p. 1 (December 2025)
[62] Sauli Niinistö, p. 42 (30 October 2024)

yet, steps should be taken to ensure robust resistance to the potential for an attack such as nets, while defence and security forces should deploy anti-drone capabilities near critical infrastructure.

What should not be overlooked is the role the State must play in security for critical assets as a societal priority – not just the sector. As a practical example, security-related costs for a fleet of tens of gigawatts already amount to tens of millions of euros per year for physical protection and cybersecurity alone. For critical facilities, these costs represent an even more significant share of their annual operating budgets. This order of magnitude demonstrates that defence-driven obligations must be assumed by the State, as imposing them on utilities would be financially unsustainable.

Considering the range, scale and increasing frequency of hybrid threats in the EU, it is imperative that Member States and power companies take steps today to make their energy assets more secure. It should not and cannot wait for a massive attack before action is taken. A preparedness culture is a necessity against the backdrop of this new normal. Therefore, the next section looks at the provisions already in place, including government policies and power companies' own actions, and benchmarks them against the new threat landscape.

02. Benchmarking preparedness in Europe's power sector

European energy security policies and legislative framework

Russia's full-scale invasion of Ukraine not only disrupted energy flows, but also fundamentally reshaped European thinking on energy security. Beyond manipulating energy supplies to Europe, Russia has deployed a hybrid toolkit including cyberattacks, sabotage of critical infrastructure, maritime interference and disinformation campaigns targeting public trust.[63]

In response, the European Commission, through its European Preparedness Union Strategy, has moved toward a more systemic and organic approach to preparedness. Alongside supportive legislation, the strategic architecture recognises that modern energy systems, characterised by digitalisation, electrification, cross-border interconnection and increased decentralisation, are vulnerable to cascading failures when confronted with security threats, such as hybrid attacks.[64] Utilities, which operate most of Europe's critical infrastructure, should therefore become co-architects of European resilience and preparedness.

The EU's preparedness architecture: legislation and key instruments

The legislative framework for the EU's preparedness and resilience towards security threats is composed of diverse instruments and pieces of legislation.

General preparedness

The European Commission's Preparedness Union Strategy (2024) represents a comprehensive strategy and a major conceptual shift from past legislative initiatives in the field of security. It embeds preparedness 'by design' into EU policies and mandates an integrated all-hazards, whole-of-government and whole-of-society approach. It also calls for minimum preparedness

[63] *Ibidem*

[64] European Commission, p. 2 (26 March 2025)

requirements, EU-level stockpiling strategies where necessary (mainly health-related goods and critical raw materials), regular stress tests and improved civil-military coordination.[65] For utilities, the message is clear: preparedness is not a technical niche but a shared responsibility between operators and public authorities.

As part of the legislative framework of the EU, the Critical Entities Resilience (CER) Directive (2023) (Directive (EU) 2022/2557) focuses on physical, operational and all-hazards resilience.[66] It requires Member States to carry out national risk assessments to identify 'critical entities' in the electricity and gas sectors, such as transmission and distribution system operators (TSOs and DSOs, respectively), generators, liquefied natural gas (LNG) terminals and interconnectors. These 'critical entities' may then be subject to obligations to conduct all-hazard risk assessments, identify cross-border and supply chain dependencies, implement resilience plans covering prevention, response and recovery, strengthen the physical protection of critical sites, coordinate with competent national authorities and report disruptions within defined timelines. As implementation is still ongoing, the practical scope and application of these obligations remain to be seen.[67]

CER is transformative because it recognises that hybrid attacks often begin with physical intrusion, cable sabotage or telecom disruption. It came into force in January 2023, but numerous Member States did not meet the October 2024 deadline to transpose it in national legislative frameworks. Consequently, progress across Europe's power sector remains a patchwork of different levels of preparedness, with TSOs and DSOs respecting different levels of guidance depending on their country.

General cybersecurity

Entering into force in 2023, the Network and Information Systems 2 Directive (Directive (EU) 2022/2555) – or NIS2 – represents a core legislative initiative for cybersecurity in the EU, establishing rigorous cybersecurity requirements for essential and important entities in the energy sector.[68] NIS2 is risk-based, requiring operators to implement "appropriate and proportionate" measures in: risk assessment and vulnerability management, segmentation between operational technology (OT) and information technology (IT) and access control, supply-chain security, detection, logging and monitoring, encryption and authentication, incident response and continuity besides rapid reporting of major incidents within 24 hours.[69]

Implementation of the NIS2 Directive is supported by the technical guidance provided by the European Union Agency for Cybersecurity (ENISA) which was established by the EU Cybersecurity Act of 2019, the Cyber Crises Liaison Organisation Network (CyCLONe), and new EU-wide detection and response mechanisms introduced by the Cyber Solidarity Act (2024).

Electricity sector preparedness

For the electricity sector, the Regulation on Risk-Preparedness in the Electricity Sector (EU 2019/941) requires Member States to prepare risk scenarios and adopt preventive and emergency plans for electricity crises.[70] It complements the CER Directive by focusing on electricity-specific

[65] *Ibidem*
[66] European Parliament, Council of the European Union (27 December 2022)
[67] *Ivi*, art. 13
[68] European Parliament, Council of the European Union, art. 21 (27 December 2022)
[69] *Ivi*, art. 23
[70] European Parliament, Council of the European Union (14 June 2019)

crisis management, ensuring that national plans address technical failures, extreme weather and cross-border disruptions. Meanwhile, the Network Code on Cybersecurity (NCCS) establishes a recurrent process of cybersecurity risk assessments in the electricity sector[71] and is a positive development towards stronger cybersecurity in the EU.

The shift of focus towards physical infrastructure security is embodied also by the growing level of coordination between the European Union and NATO, namely the Critical Infrastructure Blueprint (2024), which provides EU-NATO coordination on energy infrastructure, and the creation of the EU-NATO Task Force on Critical Infrastructure Resilience (2023). These tools signal a meaningful escalation in the European Commission's involvement in physical infrastructure security.[72]

Another layer of preparedness is represented by stress tests, which allow utilities to keep score of their level of resilience to possible attacks regularly. The European Union first adopted a system-wide framework of energy resilience stress tests in 2023-2024, which revealed gaps in cross-border coordination and recovery preparedness.[73] The Emergency Response Coordination Centre (ERCC) is also evolving into a central EU crisis hub, linking civil protection, planned military-mobility corridors and real-time monitoring.[74] For hybrid threats, the Hybrid Toolbox, which has been activated by Finland, Lithuania, Poland and Czechia after sabotage incidents, provides coordinated diplomatic, cyber, regulatory and intelligence measures.[75]

An evolving approach to electricity sector preparedness

Beyond the EU Preparedness Union Strategy, security in the electricity sector tends to be framed narrowly as security of supply, rather than as energy security in a broader sense. This prevailing interpretation focuses primarily on operational continuity and market-based solutions, particularly ancillary services designed to keep the lights on, while insufficiently accounting for physical and cyber resilience of electricity infrastructure. Expanding the definition of energy security to explicitly encompass these dimensions is therefore essential.

The 2023-24 Electricity Market Design Reform explicitly strengthens the procurement of market-based infrastructures or capabilities, which allow the system to absorb shocks and maintain operability even under cyber or physical attack. Maintaining system stability during hybrid disruptions depends on black-start capabilities, frequency containment and restoration reserves, fast-ramping generation and grid-forming inverters for renewables.[76]

Notwithstanding the importance of the market-based dimension of preparedness, utilities require advanced technical preparedness at asset level, including physical security upgrades of substations and control rooms, redundancy in telecom and supervisory control and data acquisition (SCADA), rapid restoration capabilities for transformers and long-lead components, OT visibility and monitoring, joint cyber-physical incident playbooks and hybrid-threats exercises involving law enforcement and regulators.

A useful way to frame the EU's evolving approach to energy-sector preparedness is to contrast it with the North American model. North American utilities traditionally follow a bottom-up

[71] European Commission (11 March 2024) retrieved on 23 January 2026
[72] A. Bendiek, M. Kerttunen, p. 9 (6 June 2025)
[73] S. Niinistö, *op. cit.*, p. 88
[74] *Ivi*, p. 18
[75] *Ivi*, p. 106
[76] *Ivi*, p. 98

approach: asset-level hardening, detailed technical standards and highly specialised protection measures for substations, control rooms and transmission assets. This model is comparable to State defence relying on a professional army, highly trained, technically advanced and extremely reliable in specific scenarios. Its drawback is cost: such specialised measures become prohibitively expensive to deploy across thousands of sites, particularly in distribution networks.

Europe, by contrast, has historically leaned toward a top-down approach. The EU sets broad frameworks (NIS2, CER, the Preparedness Union Strategy) and Member States implement sector-wide obligations, creating a wide but non-prescriptive umbrella covering all essential services. This resembles a conscript army, broad coverage at lower cost, ensuring that minimum standards apply to everyone, but with less precision. This is why the EU often avoids mandating highly technical stockpiling or prescriptive security upgrades and instead focuses on resilience principles, stress tests, and cross-sector coordination.

For this reason, our report adopts a balanced perspective. The top-down approach (EU legislation, national transposition, common frameworks) is essential to cast a wide net and ensure consistency. But the bottom-up approach, utilities implementing practical, technical, site-level actions, is where the most immediate gains can be achieved. Effective preparedness requires both: policy direction that ensures no critical risks are overlooked, and operator-driven measures that deliver real security outcomes at the asset level.

EU utilities' public positioning on preparedness

While EU legislation provides the overarching framework for resilience, actual preparedness depends heavily on how utilities interpret their role, evaluate risks and organise their threat response capabilities. Across the EU, the degree of risk preparedness varies, but a clear pattern is emerging. Utilities increasingly acknowledge hybrid threats and are beginning to outline the measures they are adopting to strengthen resilience and prepare in case of security risks.

A key observation is that geographical proximity to Russia influences the perception of security threats and, therefore, the level of preparedness and resilience utilities are devoting resources to. For instance, Nordic and Baltic operators are generally more explicit in discussing hybrid risks, cross-border coordination and physical infrastructure protection measures. By contrast, operators in Western and Southern Europe tend to emphasise cybersecurity, digitalisation and system governance, reflecting both different threat perceptions and different regulatory expectations.

Northern Europe

Finland is the clearest case of explicit utility-level positioning on security preparedness. The country's Total Defence model, which integrates civilian operators, government ministries, security agencies and the military, creates an environment where there is a high level of trust that utilities will participate directly in national preparedness, even though it is on a voluntary basis.[77] This approach is operationalised through the National Emergency Supply Agency (NESA), which coordinates preparedness between public and private sectors. NESA develops continuity management tools for companies, organises joint exercises with utilities and authorities and plans redundancy measures for critical information and communication systems. It also monitors international developments and maintains foreign contacts, reinforcing Finland's resilience strategy. In addition to coordination and exercises, NESA plays a central role in Finland's preparedness through the oversight of compulsory, security and emergency stockpiles, ensuring

[77] European Business Leaders' Convention, p. 17, 26 June 2025

the availability of critical inputs such as energy and fuels during major disruptions. Within the Total Defence framework, NESA also supports and steers industrial and utility production critical to military defence, in close cooperation with the Finnish Defence Forces, further embedding civilian operators into national defence readiness. The Total Defence report makes clear that energy operators are embedded into national resilience planning, including continuity of supply, cyber-physical risk assessments, cross-border coordination (notably with Estonia) and regular exercises under NESA's guidance.[78]

The Balticconnector incident reinforced public acceptance of a robust security threat preparation system. In October 2023, this pipeline linking Estonian and Finnish gas grids and providing Finland with access to Latvia's gas storage was disrupted due to external interference in the Finnish Exclusive Economic Zone (EEZ). Operators such as Fingrid, the Finnish electricity TSO, and Gasgrid Finland have openly communicated about collaboration with authorities, increased monitoring of critical assets, and the need to strengthen undersea infrastructure protection.[79] Finland therefore illustrates a case where utilities do not merely comply with EU law but are deeply integrated into State security architecture, and public disclosure is viewed as a component of collective defence.[80]

Southwestern Europe

Utilities have been more cautious in publicly discussing physical security threats, but they increasingly articulate structured cybersecurity and resilience strategies. They usually focus on governance, international standards and operational readiness rather than on specific geopolitical threats.

Iberdrola, a Spanish DSO, provides one of the strongest examples of public positioning on resilience. Its integrated report published in 2024 outlines a group-wide cybersecurity programme, including security operations centres (SOCs) and incident-response procedures.[81] Iberdrola explicitly frames cybersecurity as a core strategic pillar linked to reliability of service and regulatory compliance. Spain's high share of renewables and extensive grid digitalisation create incentives for public transparency on cyber-resilience and operational continuity.

Similarly, Redes Energéticas Nacionais (REN), the Portuguese TSO, incorporates cyber-resilience and operational continuity into its sustainability and integrated reports. The operator describes measures such as real-time monitoring and information-security certification.[82] Public reporting emphasises REN's alignment with EU legislation (NIS2, CER) and reflects a view that preparedness must evolve alongside increasing digitalisation of the electricity system.[83]

Terna, the Italian TSO, also explicitly classifies cyberattacks as a priority corporate risk, listing them alongside operational failures and extreme weather.[84] Its integrated reports detail the governance structure for cybersecurity, including risk assessments, monitoring capabilities and programme oversight by senior management.[85] Italy's system-critical role as a central Mediterranean electricity hub has led Terna to emphasise continuity of supply, resilience of substations and enhanced digital security.[86]

[78] National Emergency Supply Agency
[79] European Commission, (18 December 2023), retrieved on 1 December 2025
[80] R. E. J. Penttilä, J.Olkkonen, *op. cit*., p. 22
[81] Iberdrola, p. 112 (March 2025)
[82] REN, p. 91 (2023)
[83] *Ivi*, p. 95
[84] Terna, p. 90 (2023)
[85] *Ivi*, p. 84
[86] *Ivi*, p. 120

Central Europe

Utilities generally adopt a more explicit posture than in Western and Southern Europe, reflecting a higher perception of regional risk. ČEZ Group, a Czech DSO, stands out for its transparent discussion of cyber and physical preparedness. Its sustainability reporting describes the operation of an SOC and close cooperation with national cybersecurity authorities.[87] ČEZ also highlights investments in OT security, nuclear-facility protection and ISO-27001 certification, indicating a mature security architecture grounded in coordination with State agencies.[88]

German utilities historically publicly focus more on governance, cybersecurity and continuity planning than on physical-threat preparedness, consistent with the country's regulatory frameworks. E.ON, operating as one of Europe's largest distribution networks, also reports extensively on cybersecurity and business resilience. Its integrated report of 2023 includes sections on risk management, digital-security standards, employee training and crisis-management governance.[89] Although E.ON avoids discussing geopolitical threats directly, its public positioning clearly reflects a commitment to strengthening resilience at scale across Europe's distribution grids, where cyberattacks pose the greatest operational risk.

Analysis of utility preparedness

To better understand the bottom-up preparedness of the EU's power sector, Eurelectric conducted a series of interviews to assess the level of preparedness of European utilities, with representation from across the EU. European utilities were asked how they are preparing for crises, hybrid threats and even wartime scenarios. Through interviews and detailed questionnaires, a picture emerged of a sector that is aware of the risks but still grappling with uneven levels of readiness and the rapid change in the threat landscape they face.

General preparedness

Risk awareness is reflected in how companies assess themselves. When asked about their general preparedness as the starting point, most companies rated themselves between 6 and 8 on a ten-point scale where 1 meant preparedness was not considered at all and 10 meant they were ready for any crisis that could occur. It is important to note that responses were based on opt-in and likely favour those utilities who are already thinking about preparedness. Therefore, the results are expected to skew higher than the actual average – the overall level of utility preparedness of across the EU is likely much lower. Nonetheless, when averaged, EU utilities gave themselves a score of 6.7. The reasoning for this good, but imperfect self-evaluation is based on an evolving threat landscape. While traditional crisis plans exist, hybrid threats are exposing vulnerabilities that require new and more concerted approaches. As a result, security has climbed higher on the corporate agenda. Many respondents stress that resilience can no longer sit in isolated departments. It must be driven from leadership and embedded across all operations – an approach that many acknowledged was lacking.

A particular area where this is most notable is in equipment procurement and supply chains. Respondents repeatedly flagged chokepoints such as transformers, high-voltage equipment and specialised repair capabilities, which are indispensable and difficult to procure at speed. Many

[87] Skupina ČEZ, p. 97 (29 May 2023)
[88] *Ivi*, p. 98
[89] E.ON, p. 72 (13 March 2024)

noted that this highlights a need for stockpiling and a case for greater cross-border utility cooperation. Particularly, with the evolving threat landscape, scenarios involving coordinated or multi-station attacks are increasingly likely, and such cooperation is no longer theoretical. It becomes the decisive factor between rapid recovery and prolonged disruption.

Cooperation is not important exclusively on a utility-to-utility level either. Coordination with authorities emerged as a recurring theme, with most companies maintaining regular contact at national or local level to understand the threat landscape they face, provide information and in some cases, carry out joint exercises. However, many noted that contact with authorities is based more on personal contact, rather than formalised lines of communication, and information generally only flows in a single direction – towards authorities. This dependence on informal channels and a lack of two-way information sharing highlights a structural weakness and is fuelling calls for platforms that enable real-time intelligence sharing. The same need for structure appears internally as well: while preparedness is increasingly recognised at Board level, resistance to change and limited awareness among middle management and across departments hampers progress.

Despite these challenges, utilities point to progress worth noting. Strong governance frameworks, early adoption of technologies like drone detection and a growing security culture are sources of pride. These achievements show that resilience is no longer an abstract concept, but it is becoming an operational reality.

Current threat landscape

Preparedness alone is not enough without understanding the threat landscape. That is especially true today. As mentioned above, the preparedness utilities undertook in prior decades has rapidly become insufficient as hybrid threats increase their vulnerabilities. Companies confirmed this, reporting good situational awareness, supported by internal and external intelligence, but hybrid threats and geopolitical risks are continuing to evolve, making the unknown unknowns increasingly likely to occur with potentially calamitous consequences. To keep pace, utilities emphasise the need for continuous improvement, highlighting penetration testing and tabletop exercises as necessary parts of preparedness campaigns.

This also goes beyond company boundaries. Respondents consistently call for closer cooperation with governments, better intelligence sharing and harmonised EU-level standards for threat identification and communication. Such measures are viewed as essential for protecting critical infrastructure and ensuring access to emergency resources when incidents occur.

The urgency behind these calls becomes evident when recent experience is considered. Several companies have already faced low-level hybrid incidents, from drone incursions to cyberattacks and disinformation campaigns. While attribution remains often unclear, the conclusion is widely shared: hybrid threats are increasing, and effective monitoring must bridge both physical and digital domains.

In case of war

Turning from the hybrid threats already faced by companies to the more theoretical but not-to-be ruled out threat of full-scale war, priorities sharpen. Companies highlight in this case that people come first. There are two reasons for this. On the one hand, in case of war, human resources quickly evaporate, rightly so, as people aim to ensure personal and family security above all else. Meanwhile, energy infrastructure has been shown to be a real military target, and onsite personnel

are effectively operating on the front line. This means there is an imperative for companies to ensure workforce safety as much as possible and to not put their personnel at undue risk.

Meanwhile, companies also highlight that at the outbreak of war, there are further immediate concerns. Asset protection and continuity of service are crucial – especially given the strategic importance of power for military defence and societal continuity. Securing transformers and enhancing cybersecurity, alongside ensuring workforce safety dominate internal action plans, which manifest itself today in crisis training and logistics planning.

Running beneath all these measures is a vulnerability that unites them: communication. Utilities recognise that their ability to operate under severe disruption ultimately depends on resilient communication systems and clear protocols to maintain essential services. In the most extreme scenarios, communication is not just a support function, it is the backbone of operational survival. Inconveniently, communication often depends on access to power meaning that preparedness needs to also concern itself with ensuring robust communication in case of power outage, necessitating preparation of secure lines and backup power supplies to keep communications flowing.

03. Improving preparedness in the EU's power sector

Lessons learnt from hybrid threats and the full-scale war on the EU's border demonstrate a clear need for improved preparedness in the EU's power sector. While awareness of the threats faced is increasing, critical infrastructure is already being tested, meaning the time for action is now. Based on the benchmarking exercise undertaken in the previous section, this section makes two sets of recommendations to improve preparedness. The first are operational recommendations – steps utilities can take now to increase preparedness based on lessons learnt, best practices and gaps identified. The second are policy recommendations – three pillars to include in the EU's energy security architecture to address this new threat landscape, support utilities in their preparedness efforts and ensure we are on the same page in our efforts to mitigate the threats we face.

Operational recommendations

Already today, there are steps utilities in Europe can take to increase their preparedness. With awareness increasing that the threat landscape has changed, it is now about action. Eurelectric recommends European utilities to take steps to prepare the organisation itself, as well as its assets and the sector more broadly.

Organisational preparedness

This is an important first step to ensure that personnel and business operations are prepared for the prevailing threat landscape and are broadly 'free', requiring no or little financial commitment to realise, and should be understood as separate from defence-related functions that fall under the responsibility of State authorities. This includes:

1. **Improving situation awareness:** mapping the threat landscape faced and categorising threats based on the expected likelihood and scale of impact. These threats should include physical and cyber threats taking the geopolitical landscape into account, as well as non-malicious threats such as extreme weather, natural disasters, equipment malfunction etc.
2. **Cooperate with local authorities:** often, local authorities have a good understanding of the threat landscape, so information sharing is important. Organisations should have

formalised contact with local authorities and predefined processes for working together in case of crisis.

3. **Exercise:** awareness is the first step but drilling organisations' response to a crisis is the only way to ensure the response is effective and can be executed as planned when needed. This should be done regularly and with local authorities to ensure defined processes for cooperation.

More tangibly, organisations can act now by implementing the following:

I. **Appoint a cross-departmental anti-crisis team** in the organisation to break down information silos and have a holistic view of the organisation. The anti-crisis team should be responsible for coordinating with local authorities on a regular basis to build trust and a comprehensive threat landscape based on all possible threats – a Design Basis Threat that we expand on in the policy recommendations – including low probability high impact events such as a hybrid attack. They should then prepare clear procedures for these eventualities and with regular and realistic training exercises for the organisation. This team must include key personnel who will be responsible for taking leadership and operational roles in case of crisis.

II. **Secure communications channels and procedures** ahead of time. In case of crisis, communication equipment may be compromised due to lack of power or jammed telecommunications. Nonetheless, it is critical to ensure communication with personnel to coordinate response and recovery, remote-controlled assets to ensure continued safe operation as well as customers to maintain transparency and trust. Internally, this means preparing diverse communications equipment that can function with its own power supply and not rely on public telecommunications infrastructure. In the worst case, procedures for non-digital communication should be foreseen, while contingencies for physical control of remote-operated assets and ensuring customers receive information should be planned.

III. **Provision for employee training and safety coupled with identified capabilities for support during prolonged disruptions** to ensure they can operate with confidence in a crisis. Worst case scenario crises also mean that the workforce is likely to evaporate as individuals tend to personal and familial priorities. Ensuring the organisation can operate with minimal personnel and with the resources available is therefore crucial, meaning everyone needs to be trained to operate in a crisis scenario with a higher burden of tasks and less means to achieve them. At the same time, safety measures to shelter in place, enable remote monitoring and operation and other measures that can keep personnel out of harm's way as much as possible and maintain mental resilience should be implemented. Personal protective equipment also needs to be available for all scenarios.

IV. **Enhance supply chain resilience** by guarding against prepositioned sabotage through implementing rigorous contractor screening and adopting a 'zero-trust approach' whereby every actor is considered a potential threat, both internally and externally. Concretely, this means using the 'four-eyes' principle – where two people minimum are responsible for checking activities – should be applied for all critical work.

Asset preparedness

As crucial as the overall organisation preparedness is assets' preparedness. Resilience to attack and the capability to repair and replace damaged and/or destroyed assets is vital. This preparedness comes with more cost and should be supported by Member States as an insurance that pays off in case of crisis. To that end, a clearer distinction is needed regarding funding responsibilities across different threat environments:

- **War scenarios:** measures that fall within the remit of military defence, such as radar systems, air defence capabilities (i.e. military grade drones or missiles) or protection against advanced military threats, cannot be financed by utilities. These remain State responsibility, consistent with force-majeure principles already recognised in EU law (e.g. NIS2).
- **Below threshold security pressures:** funding should be proportionate to the assessed level of risk and supported by coordinated threat evaluations with national authorities (i.e. commercial but weaponised drones). Where additional protective measures are mandated, they should be reflected in remuneration schemes or be subsidised (especially when it affects the business case of existing assets).
- **Common operational threats:** preparedness for routine risks, such as economically motivated cyberattacks, theft or local natural events, appropriately remains within the utilities' remit and should follow a proportionality principle aligned with their capabilities and competences.

Regardless of the funding question, steps utilities can take to prepare assets for the threats identified above include:

1. **Reinforcing critical infrastructure** with physical protections, supported by Member States, especially at the points of greatest vulnerability. While it is prohibitively expensive to protect all assets, primary substations are a crucial point that can be protected with gabions, sandbags, concrete blocks and specialised nets to defend against drones – what Rasmussen Global identifies as first level protection.[90] Meanwhile, new assets should have second level protection built in with resilience by design criteria and redundancies.
2. **Stockpiling necessary equipment and repair capabilities** including particularly vulnerable system equipment that can be difficult to procure with long lead times such as transformers, as well as the means to repair assets in case of damage. This includes the workforce capabilities (skills) and support vehicles like repair vessels for offshore assets. A minimum threshold should be identified to ensure swift recovery from a worst possible case identified by a process akin to a value at risk (VaR) calculation in risk management.
3. **Cyber resilience and training by design** to stave off the bulk of attacks with clear protocols to always ensure a minimum level of cybersecurity. Simulated attacks should be rehearsed, including practicing islanding assets to contain the spread of an attack. Physical redundancies are crucial to enable islanding, and a skilled workforce is necessary to ensure response to cyberattacks is effective.

To realise these with tangible action, Eurelectric recommends utilities to implement the following:

I. **Identify and build physical protections around most critical assets** such as those that would be the hardest to recover from loss in case of an attack, such as primary substations. As mentioned, physical protections include gabions, sandbags, concrete blocks and specialised nets to defend against drones.
II. **Include 'secure-by-design' criteria in all new investments** such as hardened building material, safety provisions for personnel, built in redundancies at critical points and the potential cost of stockpiles for the most vulnerable equipment. Cyber resilience measures should also be accounted for including offline and backup systems.

[90] Rasmussen Global, p. 5 (3 June 2025)

III. **Map and stockpile necessary critical equipment** beyond transformers, where utilities should identify the chokepoints in their procurement process to better understand what presents a compounded threat in case of crisis. Equipment that is necessary for response and recovery in a short amount of time to avoid prolonged outages should be stockpiled in centres that can quickly dispatch necessary equipment when needed. Standard forms and lists should be prepared, developed by an overarching body (such as the anti-crisis team), to register critical spares, mothballed or obsolete equipment and repair capabilities. This information should be stored locally, and accessible via search function exclusively for designated government agencies in cases where damaged critical equipment requires additional spares or services.

IV. **Build strategic preparedness partnerships with other utilities** that include common stockpiles and shared repair capacities to help spread the burden across multiple parties while increasing the absolute capacity that can be procured. This could include joint exercises, as well as information sharing for security-related matters of non-commercial pertinence.

V. **Regularly review cybersecurity measures** in anticipation of a fully transposed NIS2 Directive at national level with steps such as zero-trust authentication for critical systems, strong password management, regular system updates and maintenance, as well as cybersecurity training for personnel and employing a skilled workforce to manage the cybersecurity related to critical digitalised assets.

Policy recommendations

The European Union has developed a comprehensive legislative framework for electricity system resilience, including NIS2 for cybersecurity, CER for physical and all-hazards protection, the Electricity Market Design reform for system flexibility, complemented by instruments like the Cyber Solidarity Act and the Regulation for risk-preparedness in the electricity sector. This proficiency in regulation, investment frameworks and governance structures makes the EU best placed to drive resilience across its energy system. However, legislation alone is not enough.

First and foremost, the EU and its Member States need to step up efforts of deterrence with real consequences for hybrid attacks. This is the base that determines how many threats will be faced and is critical to preventing the need for response and recovery. Meanwhile, policymakers can take steps across three areas where support is needed: implementation remains uneven, investment gaps persist and governance is fragmented. Policy must now leverage this strong foundation to accelerate delivery, secure dedicated funding, and embed integrated governance that ensures consistent standards and coordinated preparedness across the Union.

1. **Accelerate progress on legislative implementation:** the EU has introduced robust legislation for resilience, namely NIS2 for cybersecurity, CER for physical and all-hazards resilience, and EMD reform for system flexibility. However, these frameworks remain largely theoretical without timely and harmonised implementation. Fragmented national transposition creates regulatory friction and inconsistencies, while siloed approaches to cyber and physical security undermine a holistic risk management. Accelerating delivery across Member States is critical to move from theoretical compliance to real-world resilience, needed to protect critical infrastructure against evolving threats.
2. **Increase investment:** resilience is not cost-neutral. The EU needs unprecedented investment to modernise grids, strengthen cybersecurity and prepare for security threats. Without dedicated funding streams and investment frameworks, utilities cannot stockpile critical equipment, build rapid repair capabilities or deploy innovative technologies such as

redundant communication systems. Failure to invest now risks jeopardising electrification targets, increasing vulnerability to hybrid attacks and prolonging recovery times in a crisis.

3. **Improve European governance:** current governance arrangements are fragmented, with separate tracks for cyber and physical security as well as energy carriers with inconsistent standards across Member States. A holistic, EU-level framework is essential to integrate resilience into system planning, ensure coordination between authorities and operators, and provide clear guidance for both large utilities and smaller ones. By defining common threat assumptions and preparedness standards, governance can reduce fragmentation, enable joint exercises, and create a shared baseline for resilience across the Union. The boundary between energy security and national defence should also be further clarified to prevent additional defence-related criteria from imposed on existing assets during their lifetime, as well as confidential, defence-driven requirements from being imposed on utilities.

To reach these crucial targets, Eurelectric recommends adopting these practical actions:

I. **Monitor and enforce transposition with accountability mechanisms** by requiring Member States to submit quarterly progress reports on NIS2, CER, and EMD transposition, including details on designation of critical entities, risk assessments and resilience strategies. This ensures harmonisation and prevents the current fragmentation caused by 27 different interpretations of the directives.

II. **Allocate NATO resilience spending target for critical infrastructure protection** to electricity infrastructure in allied Member States. Priority areas include stockpiling high-value grid components, swift repair capabilities, robust communications and funding joint civil-military crisis exercises to strengthen coordination under hybrid threat conditions. A financial support system could be envisaged for civilian businesses within critical infrastructure sectors to offset the significant costs and efforts required for their role in national security and societal resilience.

III. **Apply 'secure-by-design' criteria to EU-funded projects and investment frameworks** by making eligibility for EU financing conditional on incorporating secure-by-design features. Projects should also include redundant communication systems (satellite/radio backups), black-start restoration capabilities and contingency protocols beyond the traditional N-1 rule.

IV. **Create a single steering group for integrated resilience planning** by mandating Member States to establish cross-functional governance bodies that unify NIS2 and CER compliance, approve joint roadmaps and coordinate hybrid exercises at least annually. This eliminates silos between cybersecurity and physical security teams and ensures a holistic risk model. At the same time, the revision of the EU's energy security architecture should also foresee greater cooperation across the Electricity and Gas Coordination Groups (ECG and GCG, respectively) to account for the increasing interaction of the energy carriers and ensure effective system planning.

V. **Adopt and operationalise a shared Design Basis Threat (DBT) for cross-EU threats** that gathers credible hybrid attack scenarios, including tactics, tools, and operational impacts that could be used as a baseline for utility risk assessments and resilience planning for those countries needing support, with the ability to tailor it, or apply it simply as an off-the-shelf standard. Pair DBT with the Vulnerability Integrated Security Analysis (VISA) methodology to prioritise protections for substations, control centres and interconnectors.

Eurelectric pursues in all its activities the application of the following sustainable development values:

Economic Development

- Growth, added-value, efficiency

Environmental Leadership

- Commitment, innovation, pro-activeness

Social Responsibility

- Transparency, ethics, accountability

eurelectric

Union of the Electricity Industry - Eurelectric aisbl
Boulevard de l'Impératrice, 66 – bte 2 - 1000 Brussels, Belgium
Tel: + 32 2 515 10 00 - VAT: BE 0462 679 112 • www.eurelectric.org
EU Transparency Register number: 4271427696-87