eurelectric
powering people

Powering security: the NATO spending and energy resilience nexus

Eurelectric position paper

December 2025

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/2025/12.105/66

Markets & Investments Committee

Contact:
Nic Steinwand, EU Energy and Climate Policy Advisor - nsteinwand@eurelectric.org
Silvia Cossa, Markets and Customers Intern – scossa@eurelectric.org

Powering security: the NATO spending and energy resilience nexus

A Eurelectric paper

December 2025

KEY MESSAGES

- **Energy security is an indispensable component of national and collective defence**, and NATO's target to allocate up to 1.5% of GDP to defence-related investments provides a critical opportunity to strengthen the resilience, protection and preparedness of Europe's energy systems.
- **Crisis management and preparedness measures**, including stockpiling critical components, enhancing repair and reconstruction capabilities, and conducting regular joint crisis exercises, **are essential to ensuring rapid recovery and continuity of energy supply during hybrid or kinetic attacks.**
- **Protecting critical energy infrastructure requires both immediate tactical defences and long-term strategic safeguards**, combining physical protection, cyber resilience, redundancy, drone-defence tools and "secure-by-design" principles integrated from the earliest stages of planning and development.
- **Robust cybersecurity and secure, independent communication systems are vital to protecting energy operations**, countering misinformation, supporting remote management, coordinating emergency responses and strengthening cooperation between private operators, public authorities and military actors.
- **Prioritising clean energy, electrification and resilient infrastructure within the 1.5% defence-related investment reinforces Europe's strategic autonomy**, reduces exposure to hostile fossil-fuel dependencies, enhances societal resilience and aligns defence imperatives with long-term competitiveness and sustainability goals.

Powering security: the NATO spending and energy resilience nexus

Context and rationale for prioritising energy investments in NATO's 2025 Defence Funding Framework

Faced with a changing geopolitical order, North Atlantic Treaty Organization (NATO)

members took a firmer commitment at the 2025 NATO Summit in The Hague: investing 5% of national gross domestic product (GDP) each year on core defence requirements and expenditures stringently related to defence and security, with the deadline to reach such a threshold set for 2035. The 5% will be composed of two elements: 3.5% of GDP devoted to core defence requirements and to meet the NATO Capability Targets. The second component will account for up to 1.5% for defence-related investments, including cybersecurity, critical infrastructure protection and crisis preparedness.

The choice adopted by NATO members represents a milestone for the energy sector in the EU: in numbers, EU GDP in 2024 corresponded to around €17 trillion. 1.5% of this and excluding unaligned Austria, Cyprus, Malta and Ireland leaves €250 billion, of which a part can and should be allocated to protecting critical energy infrastructure and ensuring the safety of the energy system of the European Union.

Russia's full-scale invasion of Ukraine has demonstrated that protecting energy infrastructure is a strategic priority as energy and particularly electricity is the backbone of a functional modern society. What it has also shown is that clean energy is more secure energy. Traditional thermal power plants (TPPs) represent large capacities that are easy to knock offline when targeted, while the distributed nature of renewables and, in principle, the protection of nuclear power plants (NPPs) under the expanded Geneva Convention[1] has made them more resilient by turning Russia's attention towards their supporting infrastructure.[2] Meanwhile, the longer that Europe relies on imported fossil fuels, the longer we continue funding the Russian war machine, further compromising our security.

Given this background and considering that the energy sector acts as the second line of defence behind the military for civil society, energy-related projects that bolster resilience should be explicitly included in the 1.5% defence-related investment. Prioritising energy investments, and particularly clean energy and electrification, strengthens the resilience of society, as reiterated in an open letter from senior military and defence experts to NATO member Heads of Government[3], while also supporting the transition to cleaner energy and enhancing Europe's strategic autonomy and competitiveness.

Eurelectric emphatically supports NATO members' decision and stands ready to provide its expertise in identifying the most strategic allocation of the 1.5% defence-related investment. Therefore, in this paper we highlight areas to be considered as part of the 1.5% figure.

1. Crisis management and preparedness

A sound and secure energy system starts at the preparation level: focusing on crisis management and preparedness ensures resilience and robustness of the European energy system during times of crisis.

[1] Additional Protocol II of 1977, Article 15 (p. 320)
[2] While the Zaporizhzhia Nuclear Power Plant has been occupied and supporting infrastructure has been targeted in attacks, direct attacks on NPPs nonetheless carry a degree of deterrence not applicable to other TPPs
[3] https://councilonstrategicrisks.org/wp-content/uploads/2025/10/Energy-Security-Open-Letter-October-2025.pdf

Financing the **stockpiling of critical equipment and spare parts** is pivotal to ensure a reactive response in times of emergency. As violently demonstrated by Russian attacks on energy infrastructure, some power plants contain fragile components which are essential to their functioning, making a stockpile of spare components crucial. A relevant example is represented by hydropower plants, where transformers, isolators and cables are fragile parts requiring spare stockpiles.

While avoiding an attack is preferable, 100% fail-safe protection is impossible. Therefore, companies should also focus on preparing for swift recovery. In this sense, funds should be devoted to **building repair and rebuilding capabilities**, alongside planning and ensuring financing for new equipment. Moreover, establishing emergency protocols is crucial and can be achieved through system redundancy, adoption of dual-fuel technology, localisation of energy storage and segmentation of the grids.

Going beyond the traditional N-1 security rule should be considered: spreading the risk across redundant components, especially those with the highest system impact, strengthens overall resilience. Distributed energy resources (DERs) particularly should be included. To cite an example, solar panels are resilient to physical attack but are rather vulnerable to cyber threats, emphasising the need for integrated cybersecurity measures as part of the N-1 rule.

Regular joint crisis management exercises involving energy companies, local authorities, emergency services and national security actors are an effective way to strengthen preparedness. These simulations typically address scenarios such as cyberattacks on critical infrastructure, large-scale power outages and physical sabotage. Their purpose is to test coordination, communication protocols and recovery capabilities under pressure. Continuing such exercises are crucial, since they significantly enhance readiness and build trust between public and private stakeholders.

Nonetheless, **cooperation between private companies and public authorities** can be sensitive, requiring secure communication channels that come at a cost. On the private companies' side, they should engage with local authorities to assess security needs while supporting endeavours towards improving resilience. From the perspective of the public authorities, they must coordinate recovery and allocate partner support. This collaboration would prove essential in case of attack, where companies could compile a list of damages after attacks and report to the public authorities to facilitate rapid repair and reconstruction with specialised response teams.

Several measures can already be put into practice to strengthen crisis management and preparation, such as:

- Companies can start **assessing which components are most fragile or critical** (i.e. transformers, isolators, cables in hydropower plants).
- **Planning and coordination** among energy companies for spare parts management and logistics.

- **Establishing emergency protocols** (redundancy, dual-fuel use, localised storage, segmentation of grids) can begin through organisational measures and regulatory support.
- Begin **risk mapping and identification of high-impact system elements** to go beyond the N-1 rule.

Other measures will require dedicated funding to be effectively implemented, including:

- **Financing the stockpiling** of critical equipment and spare parts.
- **Building and training repair/rebuilding capabilities**, including specialised maintenance teams and facilities.
- **Upgrading technologies** for dual-fuel systems and grid segmentation where capital investment is needed.
- **Support for integrated cybersecurity systems** protecting both physical and digital assets.

2. Protection of critical infrastructure

The energy sector serves as the second level of protection after the military: electricity and heating are vital, and energy infrastructure must be safeguarded against missile strikes, drone attacks, artillery and occupation in times of war, and sabotage, terror attacks and criminal activity in peace time. Protection can be conceived as two levels: first-level immediate tactical protection, such as gabions, sandbags, concrete blocks and nets to defend against drone grenades, and second-level strategic safeguarding of critical equipment. Both levels require investment to be effective.

As the Russian attacks on Ukrainian energy infrastructure have demonstrated, some power plants cannot be fully protected due to multiple factors, such as their size. Specifically, this applies to wind and solar parks, hydropower plants and nuclear powerplants. Due to this, **fortifications** such as sandbags, gabions and concrete barriers are necessary to protect the most crucial elements and components. In the case of wind and solar panels, nodal substations are crucial to protect, due to their role of transmitting produced energy to the grid. In the case of nuclear power plants, alongside nodal substations, the auxiliary systems, which guarantee the reactor is properly cooled, are essential to protect.

An increasingly common contemporary battlefield tactic is the use of drones, for which protection should be guaranteed regarding energy infrastructures. **Drone detection and influencing capabilities** must be financed, allowing companies to spot and disrupt hostile drones before they can damage critical energy facilities. While full-scale anti-drone defences are often too costly, tools like radio jammers and electronic warfare systems provide a practical way to block or misdirect drones, reducing the risk of power outages or explosions.

A pivotal role for the protection of energy infrastructure is represented by **shelters**, to be employed for maintenance, repair and crisis operation. Shelters, such as underground bunkers or mobile concrete shelters, are essential for the protection of personnel: staff working on the site of powerplants must be protected from unexpected attacks, and, when possible, shelters could be employed to manage the station remotely through digital

systems.

Strategic allocation of resources is essential. Investments should focus on the highest-risk elements, combining physical protection, cyber safeguards, stockpiling of spare parts, redundancy and coordinated exercises with military and public authorities. This integrated approach ensures that critical infrastructure remains operational under stress, enhancing resilience and stability of the European energy system.

Integrating security considerations – particularly in the face of mounting hybrid threats and lessons from the war in Ukraine - from the earliest stages of infrastructure planning and design is essential. Applying a "secure by design" approach ensures that new and retrofit energy projects are inherently resilient against physical and cyber threats. In practice, this means incorporating protective measures such as blast-resistant enclosures, drone shielding and redundant communication systems, including satellite and radio backups, from the outset. Equally, cybersecurity must be embedded in system architecture through robust access control, secure network segmentation and continuous real-time monitoring. This proactive approach not only reduces vulnerabilities and lifecycle costs but also strengthens operational continuity and overall system resilience.

A number of actions can be readily implemented to ensure the protection of critical infrastructure, including:

- Integrate novel **security considerations early** in infrastructure design ("secure by design" approach).
- **Identify and prioritise** the most critical components and high-risk elements where external actions can exploit choke points in the energy system (e.g. nodal substations, auxiliary cooling systems, critical components like inverters).
- **Coordinate with military and public authorities** for risk assessment and joint protection planning.
- Apply **cybersecurity best practices**: access control, network segmentation, real-time monitoring

Certain actions will depend on targeted financial support, such as:

- **Physical protection measures** such as gabions, sandbags, concrete barriers and nets for key assets.
- **Drone detection and counter-drone systems** (jammers, electronic warfare tools).
- **Shelters and bunkers** for staff safety and remote operation during crises.
- **Stockpiling and redundancy investments** to ensure operational continuity after attacks.
- **Implementation of "secure-by-design" upgrades** for hybrid threats (blast-resistant structures, redundant communications, satellite/radio backups).

3. Cybersecurity and communication

Secure and effective communication is an essential part of the protection of energy infrastructure, from carrying out remote operation of energy infrastructures, managing emergency situations, delivering crucial updates, coordinate emergency responses and nurturing trusting relations with relevant stakeholders.

Due to their importance, **connection and communication methods must be independent and safe**, and it could be managed through satellites, Global System for Mobile Communications (GSM), Fiber and radio.

Cybersecurity is also a crucial aspect of safeguarding energy infrastructure, complementing physical security measures. Misinformation and fake news can directly threaten operations by undermining trust, discouraging support, stirring unrest, or disrupting energy markets. Devoting funds to cyber protection is essential because investing in proactive communication strategies, such as transparent public engagement, maintaining and providing real-time information to consumers can prevent these risks from escalating into operational or financial crises. Allocating resources ensures that companies can effectively counter misinformation while coordinating with governments and platform regulators, ultimately protecting the stability, reliability and reputation of energy systems.

In high-risk environment, close **cooperation with military authorities** is essential for ensuring the safety and resilience of energy infrastructure. Joint exercises and coordinated procedures allow energy companies and armed forces to respond quickly and safely after possible attacks, including inspecting facilities for damage, neutralising threats, and clearing hazards in reclaimed areas. Collaboration with mobile air defence teams further enhances protection, as these units can rapidly deploy anti-drone and anti-missile measures to safeguard critical energy sites. Regular exercises and operational coordination with military units ensure that energy personnel are trained, response protocols are tested, and protective measures are effective, making this partnership a crucial investment in energy security.

Immediate steps can be taken to improve crisis readiness and ensure the robustness of the energy system, for instance:

- Establish **secure communication protocols** and coordination procedures between energy operators, authorities, and military units.
- Use **existing channels** (satellite, GSM, fiber, radio) to ensure communication redundancy and reliability.
- **Conduct joint exercises** with military and emergency services to test response and coordination.
- **Implement proactive communication strategies** to counter misinformation through transparency and timely updates.

Specific initiatives will require additional investment to ensure their successful deployment, namely:

- **Investment in secure, independent communication infrastructure**, including satellite and radio systems resilient to disruption.
- **Cybersecurity enhancements** to protect networks, data, and communication channels from attacks.
- **Dedicated funds for counter-misinformation efforts**, real-time public information systems, and coordination with regulators.

Financing for joint training and rapid-response cooperation with military and mobile air defence units.

Conclusion

The evolving geopolitical landscape underscores the critical importance of investing in energy security and the protection of energy infrastructure. Strategic allocation of the 1.5% of GDP to defence-related investment offers a unique opportunity to strengthen resilience, enhance cybersecurity, safeguard critical assets and ensure rapid crisis response across Europe's energy system. Eurelectric remains committed to advocating for the prioritisation of energy-related projects within this framework and will continue to provide expertise and guidance to ensure that these funds are used effectively to protect infrastructure and reinforce Europe's strategic autonomy.

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

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