EUROPEAN POLICY CENTRE

DISCUSSION PAPER

EUROPE'S POLITICAL ECONOMY PROGRAMME

27 NOVEMBER 2026

Blackout continent:

12 recommendations for securing Europe's energy systems

Georg Riekeles
Varg Folkmann
Philipp Lausberg



Credit: NASA 2024

Table of contents

Executive summary 3

Europe's new energy security reality 4

The energy transition and Europe's evolving vulnerabilities 5

What is secure and resilient enough? 6

Going forward: 12 priorities for energy infrastructure security 7

I) Assess system risks and define required resilience 9

II) Invest in resilient infrastructure and recovery capacity 10

III) Organise crisis cooperation and response 10

Conclusion 11

Endnotes 12

ABOUT THE AUTHORS



Georg Riekeles is Associate Director and Head of Europe's Political Economy Programme at the European Policy Centre.



Philipp Lausberg is a Senior Policy Analyst in the European Political Economy Programme at the European Policy Centre.



Varg Folkman is a Policy Analyst at the European Policy Centre Europe's Political Economy Programme.

ACKNOWLEDGEMENTS / DISCLAIMER

This Policy Brief forms a part of the EPC's work on the EU's economic security under the *Brussels Economic Security Forum*. It is the product of two dedicated roundtables held in 2026 on 'Protecting Europe's Energy Infrastructure' and 'Securing Europe's Energy Supply in a World of Rupture' followed by interviews and discussions with policymakers, industry practitioners and experts.

The EPC is grateful for the involvement of its partners, in particular the support and knowledge partnership with DNV. The support the European Policy Centre receives for its ongoing operations, or specifically for its publications, does not constitute an endorsement of their contents, which reflect the views of the authors only. Supporters and partners cannot be held responsible for any use that may be made of the information contained therein.

Executive summary

Europe's energy security is no longer only a question of securing affordable energy supplies. Russia's war against Ukraine, disruptions to global energy flows and attacks on critical infrastructure have exposed vulnerabilities spanning physical assets, digital control systems and dependencies on specialised equipment and repair services. The shift towards electrification and domestic clean energy generation can reduce dependence on imported fuels but also increases the importance of resilient electricity infrastructure.

EU legislation, including the Critical Entities Resilience Directive, NIS2 and sectoral preparedness rules, provides an important foundation. Yet fragmented risk assessments, unclear responsibilities, limited repair capacity and insufficient coordination between operators, governments and security institutions leave gaps in Europe's ability to withstand complex or sustained disruptions.

This Discussion Paper proposes **12 recommendations across three priorities**:

1. **Assess system-wide risks and define resilience requirements:** Integrate physical, cyber and supply-chain risk assessments; map essential functions and critical dependencies; establish measurable standards of what is "secure enough" for maintaining and restoring essential services; and address dependencies throughout the asset lifecycle.
2. **Invest in resilient infrastructure and recovery capacity:** Embed security and repairability into new projects; secure strategic stocks and shared repair capabilities; strengthen pipeline protection; and establish appropriate public–private cost-sharing arrangements for security and resilience.
3. **Strengthen crisis cooperation and response:** Clarify public and private operational responsibilities, improve emergency procedures and contracts, deepen EU–NATO cooperation drawing on Ukraine's experience, and ensure credible responses to hostile action.

Europe cannot prevent every disruption. The essential challenge is to determine what level of resilience is sufficient, who is responsible for delivering it and how its costs should be shared. The forthcoming EU energy-security framework revision offers an opportunity to turn fragmented preparedness requirements into coordinated, tested capabilities.

Europe's new energy security reality

The 2020s have seen a succession of energy crises hit Europe. Russia's full-scale invasion of Ukraine and the subsequent collapse in Russian gas deliveries drove up prices and forced governments to scramble for alternative supplies. The disruption of energy flows through the Strait of Hormuz in 2026 brought a further reminder of the insecurity that comes with dependence on imported fuels. Diversification has helped Europe weather these shocks, but it cannot insulate the continent from disruption elsewhere in the global energy system.[1]

Closer to home, damaged subsea connections and warnings of sabotage have exposed the vulnerability of the infrastructure through which energy reaches households and businesses. National security services have explicitly identified energy infrastructure as a potential target and warned about reconnaissance of critical assets.[2] The question facing Europe is increasingly whether it can keep its energy system functioning when parts of it come under sustained pressure.

This requires energy infrastructure security to encompass three interdependent dimensions: physical security, cybersecurity and security of supply, including access to equipment, spare parts, maintenance and repair services. A cable can be protected against physical interference yet remain vulnerable through its control systems. An installation that survives an attack may still be unusable if the components or expertise needed to restart it are unavailable.

Europe will never attain absolute energy security, as interconnected energy systems remain exposed to evolving threats, and not every disruption can be prevented. It must therefore decide ***what is secure and resilient enough***: which risks it can bear, which functions must be preserved and how quickly disrupted services must recover. There will be costs, both in expanding infrastructure and in making it resilient. The cheapest system to build may prove expensive to restore. Building on the EPC's earlier call for comprehensive energy system risk management, this brief discusses ideas for what a coordinated approach to protection, preparedness and recovery must look like.[3] The forthcoming revision of the EU energy-security framework is an opportunity to confront these choices, within a wider agenda of infrastructure investment, preparedness and security cooperation.

Figure 1

DAMAGE TO SUBSEA CABLES AND PIPELINES IN THE BALTIC SEA SINCE 2022



Source: Wilson Centre, Mapping Undersea Infrastructure Attacks in the Baltic Sea.

The energy transition and Europe's evolving vulnerabilities

Europe's response to energy insecurity has long centred on obtaining sufficient supplies at affordable prices. The 2017 Security of Gas Supply Regulation and the 2019 Electricity Risk-Preparedness Regulation established cooperation and planning arrangements. After Russia's invasion of Ukraine, emergency measures, gas storage requirements and supply diversification helped avert more severe shortages. Yet the need for additional legislation during the crisis that ensued showed that the existing framework was insufficient to deal with the pressures it faced.[4]

The longer-term response involves changing how European countries produce and use energy. Decarbonisation can strengthen security, provided investment in generation is matched by the networks, flexibility and storage capacities needed to deliver reliable power.[5] Expanding domestic clean energy generation and reducing energy demand through greater efficiency in buildings, industry and transport offer a route towards lower exposure to imported fuels. Renewables accounted for approximately 47% of EU electricity generation in 2025, but only 26% of overall final energy consumption.[6]

Electricity itself represented just 23% of final energy consumption in 2024, highlighting the need to accelerate electrification alongside the expansion of renewable generation.[7]

Moving towards a more electrified system requires more than installing solar panels or putting wind turbines in the Baltic Sea, and ambitious electrification objectives raise the stakes of infrastructure security. Producing power in one part of the Union helps consumers elsewhere only if it can be moved to where it is needed. New connections can provide alternative routes during disruption, while decentralised generation can reduce dependence on individual plants. These benefits depend, however, on planning the system as a whole.[8]

Moving towards a more electrified system requires more than installing solar panels or putting wind turbines in the Baltic Sea, and ambitious electrification objectives raise the stakes of infrastructure security.

A working example is the Baltic states' synchronisation with the continental European electricity grid in February 2025. Following joint grid upgrades, contingency tests and coordination among Baltic and Polish transmission system operators (TSOs), Estonia, Latvia and Lithuania ended their reliance on Russian-controlled frequency management. EU funding and ENTSO-E cooperation helped make this a concrete gain in energy independence and operational resilience.[9]

The transition also changes Europe's external dependencies. In 2024, China supplied 98% of the value of the EU's solar-panel imports from outside the Union.[10] This concentration presents Europe with difficult choices. Low-cost imports help projects proceed, but the immediate savings must be weighed against the exposure created over an installation's lifetime. For equipment that requires remote updates, proprietary software or specialist maintenance, the commercial relationship can create dependencies lasting decades.

Related cyber vulnerabilities extend across the energy technology stack: from firmware in inverters and substation equipment to operational control systems, interfaces between corporate IT and operational technology (OT), and suppliers' remote-access, cloud and software-update services. The key question that so far has been insufficiently explored is who can access, manipulate or disable critical functions.

The key question that so far has been insufficiently explored is who can access, manipulate or disable critical functions.

EU infrastructure policy has gradually caught up with this changing environment. The 2008 European Critical Infrastructure Directive focused on energy and transport. Its 2022 successor, the Directive on the Resilience of Critical Entities (CER), covers eleven sectors and addresses continuity of essential services across natural and human-made hazards.[11] NIS2 strengthens cybersecurity obligations, including supply-chain risk management.[12] An electricity cybersecurity network code, in force since June 2024, adds rules for cross-border flows.[13]

Together, these instruments recognise that infrastructure security reaches beyond the perimeter of an individual facility. The remaining task is to turn that recognition into reliable performance under pressure. Much of the infrastructure being built today will remain in service for decades. Decisions about design, location and suppliers will shape Europe's options long after the initial investment has been recovered. Security requirements established now can prevent vulnerabilities that would otherwise become expensive to remedy.

What is secure and resilient enough?

A secure and resilient energy system must be able to preserve vital functions when something goes wrong. That sounds straightforward until the choices become concrete. How long can a region manage without an interconnector? Which services receive priority during restoration? How much spare equipment should an operator keep in reserve for an incident that may never occur? And who pays when an investment in one country primarily protects consumers or essential services in another?

No one can promise uninterrupted operation in every circumstance. Nor can resilience rest solely on estimates of attack probability, which are uncertain and change as adversaries adapt. The World Economic Forum's *Risk Management, Reimagined: Outlook to 2035* argues that risk management must increasingly prepare organisations for unpredictable events drawing on continuous monitoring and intelligence to integrate risk management closer into strategic decisions.[14] It does not make specific risk assessments redundant but explains that assessments must try to gauge capabilities when the actual disruption differs from the anticipated scenario.

For energy systems, this means using resilience criteria to shape infrastructure, supplier and investment choices, then regularly testing whether their underlying assumptions still hold. Beyond a minimum level of protection for essential functions, additional measures should be judged against the disruption they can prevent or shorten, including consequences that fall outside an operator's balance sheet.

Existing legislation provides a foundation. CER required member states to identify critical entities by July 2026; those entities must assess their risks and take proportionate resilience measures. Commission guidance issued that same month addresses technical, security and organisational measures.[15] NIS2 and the electricity cybersecurity network code address digital vulnerabilities. However, compliance with separate obligations does not establish whether the people, equipment and authority needed for a combined crisis will all be available at the same time when the time comes.[16] A company can have a business-continuity plan without knowing whether its communications provider will remain operational. A country can plan to draw on neighbouring supplies without accounting for a disruption that affects both sides of the border. These are failures of coordination that individual compliance cannot resolve.

A concrete example is the coordinated cyberattack on Poland's energy infrastructure in December 2025. Attackers targeted at least 30 wind and solar farms, damaging control systems and disrupting communication with distribution network operators. Although electricity generation continued uninterrupted, the incident demonstrated how compromised industrial equipment and software can undermine operators' ability to monitor and remotely control critical infrastructure.[17]

EU risk assessments are already organised at several levels. System risk assessment and readiness is the practical test the next phase of policy must meet. Under CER, national all-hazards assessments guide

Table 1: Who assesses which risks, and who acts on the findings?

Assessment level	Existing responsibilities and purpose
Critical entities and national essential services	Under CER, member states assess risks to essential services and identify critical entities. Those entities assess their own risks and dependencies and implement proportionate resilience measures.
Electricity and gas systems	National competent authorities, regional cooperation arrangements and European network bodies develop crisis scenarios, risk assessments and preparedness plans under sector-specific rules.
Cross-border electricity cybersecurity	The electricity cybersecurity network code provides for entity, national, regional and Union-level assessments, with distinct roles for competent authorities, ENTSO-E, the EU DSO Entity, ACER and ENISA.
EU economic security	Commission and member-state assessments examine strategic dependencies and economic-security exposure. They inform broader policy choices, rather than constituting another level of operational crisis planning.[18]

the identification of critical entities, which then assess their own vulnerabilities. For electricity, ENTSO-E's regional crisis scenarios inform national preparedness plans. The electricity cybersecurity network code adds Union-wide, regional, national and entity-level assessments of digital processes affecting cross-border flows.

The challenge is to connect these findings to joint investment priorities, operational responsibilities and tested recovery plans.[19] An operator's recovery plan may depend on communications, neighbouring supplies or repair resources that are also needed elsewhere. Joint assessments must test whether such assumptions would remain valid in the event of a shared disruption. ENTSO-E's call for integrated assessments, clearer crisis responsibilities and coordinated restoration underlines the need to connect existing processes.[20] Responsibility must extend beyond compiling a consolidated picture to ensuring that material gaps are addressed.[21]

The most vulnerable points are often the seams and nodes where systems and responsibilities meet: landing stations, substations, compressor stations, ports and control centres, or the links between electricity, telecommunications and transport. A modest installation can support a major cross-border supply route. Conversely, a large asset may have workable substitutes. Criticality therefore depends on consequences, alternatives and restoration time. A static national list cannot capture every changing regional dependency.[22]

The most vulnerable points are often the seams and nodes where systems and responsibilities meet: landing stations, substations, compressor stations, ports and control centres, or the links between electricity, telecommunications and transport.

This matters particularly for repair. Some energy infrastructure involves heavy, bespoke equipment that cannot readily be substituted. Specialised refinery components, landing facilities and remote installations can be difficult to restore even when the damage itself is understood. Telecommunications equipment is often more standardised, but cable location, vessel availability and access can delay recovery in either sector. Standards can improve interchangeability; they cannot supply a missing vessel, manufacture a component overnight or ensure that several operators have not booked the same scarce resource.[23]

Supplier dependencies add another complication. Reliance on imported panels differs from reliance on equipment whose settings can be changed remotely. The relevant questions are who can access the controls, withdraw maintenance, interrupt updates or enable restoration. An inexpensive component can become a costly vulnerability if only its original manufacturer can service it. Cybersecurity routines and stocks may mitigate some risks; others require a different supplier or system design. Security assessments must follow the asset through its operating life. The same logic applies to operational knowledge. Access to spare parts is of limited value if the engineers needed to install them are unavailable or if replacing the supplier means losing access to essential software. Preserving the capacity to maintain and restore infrastructure deserves the same attention as diversifying the equipment initially purchased.

The March 2025 Preparedness Union Strategy places such questions in a broader setting. It promotes preparedness by design, stockpiling, public–private emergency protocols and civilian–military cooperation.[24] This is particularly relevant to energy: hospitals and communications need electricity, while restoring electricity depends on communications and transport. Yet cooperation can fail for mundane reasons. The necessary company representative may lack security clearance; a repair contractor may lack access; a contract may leave responsibility disputed. Preparedness must address these obstacles before an incident.

More targeted initiatives show how the wider strategy can translate into action. The February 2025 EU Action Plan on Cable Security covers both power and data cables across prevention, detection, response, recovery and deterrence. The subsequent risk assessment and February 2026 Cable Security Toolbox provide a more detailed basis for implementation.[25] Pipelines fall within wider energy and resilience arrangements, but there is no equivalent dedicated pipeline-security action plan among these initiatives. A focused programme could address the specific interfaces between surveillance, intervention, repair and alternative supply, particularly for routes connecting the EU with neighbouring partners.

Investment policy is also changing. The Council's June 2026 negotiating position on the European Grids Package proposed a priority category for the security and resilience of existing electricity infrastructure, which would make critical components for emergency repairs of electricity interconnectors eligible for EU funding.[26] The case for such support is strong: Operators may have little commercial incentive to invest in additional redundancy, spare equipment or repair capacity when much of the benefit accrues to consumers in other countries, essential public services or defence. Public support can help address this gap where resilience provides wider societal or cross-border benefits. Better information makes for better decisions, particularly information about system dependencies and available resources, shared through arrangements that protect sensitive details.

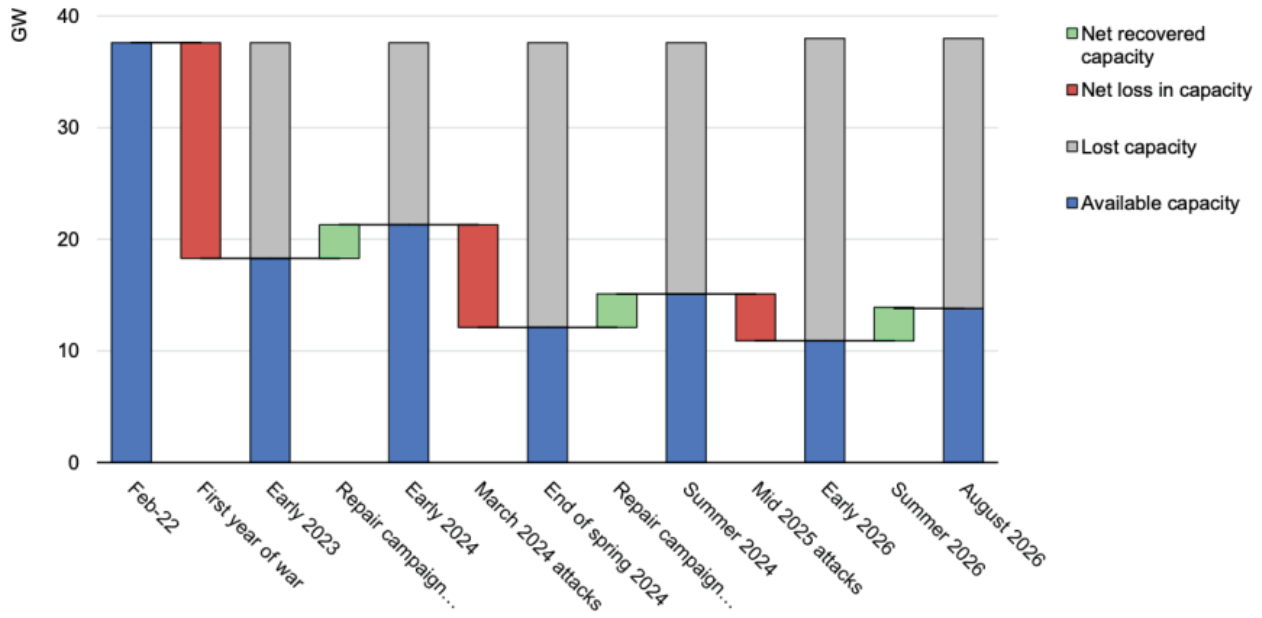
The forthcoming energy-security framework revision should bring these initiatives together through coherent gas and electricity preparedness, incorporating physical, cyber and supply-chain risks. While it cannot, by itself,

settle every issue of industrial capacity and contractual authority, the review provides an opportunity to adapt supply-security rules to a more electrified and interconnected system.[27]

Hostile action raises additional questions of surveillance, civilian–military cooperation, attribution and response. The EU–NATO infrastructure assessment and NATO's Baltic Sentry already provide foundations for civilian–military cooperation and maritime vigilance.[28] Their contribution must be linked to decisions and capabilities onshore. Protecting every kilometre of cable or pipeline continuously is unrealistic. A credible approach must combine selective protection with the ability to detect interference, limit its consequences and restore service. It must also avoid leaving hostile actors confident that repeated disruption carries little cost. Europe needs to know both how it will restore a damaged system and how it will respond when disruption is deliberate.

Figure 2

SUSTAINED ATTACKS: AVAILABLE DISPATCHABLE POWER GENERATION CAPACITY IN UKRAINE, 2022–26.



Source: IEA, Ukraine's Energy Security 2026: Pre-winter assessment 2026–2027.

Going forward: 12 priorities for energy infrastructure security

The next phase of European energy security should focus on whether the system as a whole can withstand disruption and recover. A shared approach to risk assessment should guide this work, connecting physical threats, cyber vulnerabilities and supply-chain dependencies across sectors and borders. Assessments must identify which functions are indispensable, how failures could spread and where protection or recovery measures would make the greatest difference. Public authorities should use these findings to define what is secure enough. Operators, supported by technical and independent assurance expertise, should demonstrate that the necessary capabilities exist and work under demanding scenarios. This provides a basis for prioritising investment, assigning responsibilities and sharing costs, while connecting civilian resilience with collective security and responses to hostile action.

The following twelve priorities span several policy instruments. The energy-security framework revision should anchor integrated assessment and preparedness. Implementation of CER and NIS2, grid investment rules,

BOX 1: METHODOLOGICAL EXAMPLE: HOW TO ESTABLISH A RESILIENT ENERGY SERVICE

For a critical connection, public authorities and private operators must aim to establish and know what service will be available during an outage, the acceptable duration of reduced supply and the resources needed to restore it. The four steps below can turn that objective into an evidence-based judgement as part of a continuous cycle.[29]

1. Assess risks and dependencies. Examine how the service could fail and whether alternative supply, communications and repair resources remain available under combined disruptions. Record uncertain assumptions.

2. Make investment priorities. Compare protection, redundancy and repair options against the agreed service and restoration objectives. Assess their cost and usefulness across several scenarios, while meeting mandatory requirements.

3. Establish effective controls. Secure replacement equipment, trained crews, contractual rights and access arrangements. Assign responsibility for maintaining each capability, rather than merely recording it in a plan.

4. Test and reassess. Exercise restoration, including loss of trusted digital control and competing demands for repair resources. Verify that the timetable is achievable, correct shortcomings and retest after material changes.

procurement and contractual arrangements must carry much of the operational work. Pipeline protection, EU–NATO cooperation and responses to hostile action require complementary initiatives. Defining clear responsibilities across these strands will matter more than placing every recommendation in one legislative proposal.

I) ASSESS SYSTEM RISKS AND DEFINE REQUIRED RESILIENCE

1. Connect risk assessments and assign responsibility for delivery

The Commission should use the framework revision to connect physical, cyber and supply-security assessments through common disruption scenarios and compatible preparedness requirements. Each member state should assign an existing authority responsibility for consolidating material cross-sector dependencies. The Commission should coordinate examination of cross-border gaps with national authorities, network bodies and operators. The output should be an agreed programme of corrective actions, with responsible organisations, funding and deadlines. Joint exercises should test whether the resulting capabilities work.

2. Map mission-critical seams and nodes continuously

Member states and operators should maintain rolling regional maps of essential functions and their dependencies. Priorities should reflect consequences, alternatives and replacement time, with particular attention to hard-to-replace components, landing facilities and remote installations. Updates should follow major network changes, incidents and new threat information. Controlled access should protect sensitive maps while allowing their findings to guide investment, stockpiling and cross-border preparedness.

3. Define performance standards that demonstrate what is “secure and resilient enough”

Public authorities should establish minimum service levels, endurance and restoration objectives. Operators and asset owners should translate these into risk-based strategies for protection, redundancy, maintenance and recovery, building on existing standards and ALARP (As Low as Reasonably Practicable) principles. This would give a better basis for investment decisions. This is a dynamic process that needs to account for changes to the threat picture.

Private technical and assurance bodies can contribute with risk assessment, process management, cybersecurity testing and independent verification. Evidence should show that people, equipment, contracts and exercises support the claimed capability. Regional testing must complement individual assessments since operators that seem resilient in isolation may still depend on the same vulnerable suppliers, infrastructure or scarce repair resources, creating system-wide points of failure.

4. Address dependencies throughout the asset lifetime

Procurement of critical energy infrastructure should assess suppliers’ remote access to equipment, risks arising from foreign laws that could restrict maintenance or support, supply concentration and substitutability throughout operation and maintenance. Requirements should include independently auditable software and firmware, operator-controlled updates and remote access, interoperable components, and the ability to operate or restore essential functions without depending on a supplier’s proprietary software, cloud services or remote support. Where critical functions cannot be adequately protected, alternative suppliers or architectures are necessary. Longer-term procurement and coordinated demand can help sustain diversified manufacturing and servicing capacity, prioritising the dependencies most capable of interrupting essential functions.

II) INVEST IN RESILIENT INFRASTRUCTURE AND RECOVERY CAPACITY

5. Build security and repairability into new projects

Major projects should demonstrate how they plan for the facilities to remain controllable, maintainable and repairable during disruption. Appraisal should cover lifetime security costs, secure digital access, alternative communications, replacement components and access for repair crews. Network design should avoid routing apparently independent connections through one vulnerable node. These requirements should inform siting and design early enough to prevent expensive retrofitting.

6. Secure strategic stocks and collective repair capacity

Regional arrangements should pool appropriate long-lead-time components and secure specialist crews, storage, repair vessels and manufacturing capacity in advance. Agreements must allocate resources during simultaneous disruptions and facilitate emergency cross-border deployment. Equipment swaps and transfers of ordering rights under existing procurement frameworks could accelerate assistance. Standardising components and repair interfaces should improve future recovery while existing assets retain technically realistic repair plans.

7. Assess the need for an action plan for critical energy pipelines

Drawing on the EU cable-security action plan and existing repair capabilities such as the PRSI Pool, the Commission and High Representative should work with member states, operators, Norway and the UK to identify gaps in pipeline protection and recovery. The assessment should consider critical routes, landing facilities and compressor stations as interconnected systems, covering surveillance, incident response, repair capacity and alternative supplies during prolonged or simultaneous outages.

Where gaps require coordinated European action, a targeted pipeline-security action plan should assign responsibilities, funding and deadlines. It should build on existing arrangements and prioritise infrastructure that will remain essential to supply security throughout the energy transition.

8. Allocate resilience costs explicitly

Regulators should allow network operators to recover efficiently incurred security and resilience costs through regulated network tariffs. However, where governments impose additional requirements for national security or defence purposes, such as enhanced physical protection, redundancy or rapid recovery capabilities for strategically critical infrastructure, the additional costs should be explicitly identified and shared with public authorities, including defence ministries where appropriate. EU funding should support investments with cross-border benefits and shared capabilities that individual actors would underprovide.

Funding should reflect demonstrable improvements in continuity and recovery, while procurement and reporting rules must protect sensitive configurations without compromising competition, audit and accountability.

III) ORGANISE CRISIS COOPERATION AND RESPONSE

9. Make public–private crisis cooperation operational

National authorities and operators should designate crisis representatives and alternates, arrange appropriate security clearances and establish secure communications and escalation procedures. Information hubs should connect surveillance and operators reporting with authorities able to act. Regular exercises must test simultaneous outages, lost communications and competition for repair resources, involving senior business leaders and producing corrective actions with

BOX 2: BEST PRACTICE EXAMPLE: THE PIPELINE REPAIR AND SUBSEA INTERVENTION (PRSI) POOL AT KILLINGØY

Recent incidents have exposed the vulnerability of Europe's tens of thousands of kilometres of subsea oil and gas pipelines that cross the North Sea and Baltic, illustrating the scale of Europe's infrastructure protection and repair challenge. Industry cooperation can turn uncertainty into preparedness and operational capacity.

The Pipeline Repair and Subsea Intervention (PRSI) Pool at Killingøy in Haugesund is an obligatory membership-based arrangement giving critical North Sea operators access to a common pool of specialist subsea repair equipment and expertise for pipelines and offshore power cables.[30] Members share the costs of maintaining equipment, trained personnel and repair arrangements, including vessel response commitments. This connects physical infrastructure resilience with the availability of essential supplies and services.

This example points towards the future of a broader European approach: mapping mission-critical assets, agreeing restoration objectives and ensuring that equipment, skills, contracts and funding can deliver them. Public authorities and operators should build on existing arrangements to identify gaps in coverage, test capacity against simultaneous disruptions and agree restoration priorities for Europe's broader critical infrastructure needs.

BOX 3: THE CASE OF UKRAINE: DEALING WITH AN ENERGY SYSTEM UNDER SUSTAINED ATTACK

Since Russia's full-scale invasion in 2022, Ukraine's energy infrastructure has faced repeated attacks on power plants, substations and transmission networks. Repaired facilities often become targets again, while increasingly sophisticated drones complicate protection and recovery.

Ukraine has responded through air defence, physical protection, rapid repairs and decentralised energy supply. Transmission system operator Ukrenergo has prioritised 18 substations critical for nuclear electricity generation, cross-border trade and grid restoration. By August 2026, around 200 protective structures had been installed, with another 280 under construction.[31]

Ukraine has also adapted to cyberattacks. During the 2015 grid attacks, operators restored power using manual controls despite compromised digital systems.[32] In April 2022, close cooperation between Ukraine's cybersecurity authorities, operators and private experts helped thwart a sophisticated attack on high-voltage substations.[33]

Distributed generation and electricity imports from neighbouring countries have further supported continuity. Nevertheless, repeated attacks and shortages of equipment and personnel continue to constrain recovery, illustrating both the adaptability and limits of energy resilience under sustained attack.

deadlines. Usable warnings should also reach relevant personnel without classified access.

10. Prepare contracts and emergency authority

Governments and operators should review emergency access, alternative maintenance, supplier withdrawal, insolvency and changes of ownership before disruption occurs. Critical contracts should provide appropriate access to documentation, software, tools and parts needed for continuity. Intervention powers, compensation, liability and expedited dispute procedures require advance clarification and legal safeguards. Exercises should establish whether those arrangements actually allow repairs to be commissioned and carried out.

11. Set practical tasks for EU–NATO cooperation

An agreed work programme should connect threat assessments, civilian–military exercises and assistance procedures for infrastructure supporting essential services and military activity. Operators retain technical responsibilities, national authorities direct interventions, EU instruments support coordination and investment, and NATO contributes relevant military capabilities. Regional arrangements should include Norway and the UK and specify who requests assistance, authorises access and coordinates restoration. Ukraine's experience of maintaining and restoring energy infrastructure under sustained Russian attacks should inform exercises and recovery planning.

12. Connect resilience with attribution and response

Operators, intelligence services and law enforcement should agree on evidence-preservation procedures and share relevant findings securely. Governments should coordinate protective action, public attribution and proportionate responses, recognising their different evidentiary and legal requirements. Immediate precautions need not await a criminal judgement, but suspicion or correlation does not establish responsibility. Credible consequences for substantiated hostile action should accompany protection and recovery, supported by public communication that explains what is known without amplifying an adversary's effects.

Conclusion

Europe cannot secure its energy future simply by changing where its fuels or equipment come from. It must be able to operate, maintain and restore the systems on which daily life depends. The central questions are what level of security and resilience is sufficient, who must deliver it and how its costs are shared. Answering them requires making choices about essential functions, vulnerable seams and nodes, and the assets hardest to replace. The framework revision can bring greater coherence to these choices, but delivery extends across investment, industry and security policy. Europe will remain exposed to shocks. It should be far better prepared to withstand them.

[1] European Commission. In focus: EU energy security explained. 20 April 2026. https://energy.ec.europa.eu/news/focus-eu-energy-security-explained-2026-04-20_en.

[2] Danish Defence Intelligence Service. Intelligence Outlook 2025. 2025, p.40 https://www.fe-ddis.dk/globalassets/fe/dokumenter/2025/-fe-intelligenceoutlook-25-.pdf; EU-NATO Task Force. Final Assessment Report on the Resilience of Critical Infrastructure. June 2023. https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf; Norwegian Police Security Service. National Threat Assessment. 2025, p. 12 https://www.regjeringen.no/contentassets/6290dec36c374ee191e5c7dbba18a258/nasjonal-trusselvurdering-2025_no_web.pdf.

[3] Świeboda P, Riekeles G, Dekeyrel S. Building *Economic Security into Europe's Clean Energy Agenda*. Brussels: European Policy Centre; 13 February 2025. https://epc-web-s3.s3.amazonaws.com/content/Building_Economic_Security.pdf.

[4] European Commission. *Commission publishes "fitness check" on EU laws covering the security of electricity and gas supply*. 5 January 2026. Staff Working Document SWD(2025) 435. https://energy.ec.europa.eu/news/commission-publishes-fitness-check-eu-laws-covering-security-electricity-and-gas-supply-view-future-2026-01-05_en.

[5] Świeboda P, Riekeles G, Dekeyrel S. *Building Economic Security into Europe's Clean Energy Agenda*. Brussels: European Policy Centre; 13 February 2025. pp. 16–18 and 27–29. https://epc-web-s3.s3.amazonaws.com/content/Building_Economic_Security.pdf.

[6] DNV. Energy Transition Outlook 2026. 2026. https://www.dnv.com/energy-transition-outlook/2026/; Eurostat. *Renewable energy and natural gas supply up in 2025*. 29 June 2026. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20260629-2; Eurostat. *Renewables make up 26% of EU energy use*. 23 July 2026. https://ec.europa.eu/eurostat/en/web/products-eurostat-news/w/ddn-20260723-1.

[7] Eurostat. *Energy in Europe – 2026 edition, interactive publication*. 2026. https://ec.europa.eu/eurostat/web/interactive-publications/energy-2026.

[8] Agora Energiewende. *Navigating energy security amid an evolving risk landscape*. 28 April 2026, Sections 3–6. https://www.agora-energiewende.org/publications/navigating-energy-security-amid-an-evolving-risk-landscape.

[9] Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities (CER Directive). https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng. European Commission. *Guidelines on the application of Article 13(5) of Directive (EU) 2022/2557*. C/2026/3712; 13 July 2026. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026XC03712.

[10] Eurostat. *EU imports €14.6 billion in green energy products*. 9 October 2025. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20251009-2.

[11] European Commission. *The Critical Entities Resilience Directive enters into application*. 23 October 2024. https://home-affairs.ec.europa.eu/news/critical-entities-resilience-directive-enters-application-ensure-protection-critical-infrastructure-2024-10-23_en.

[12] Directive (EU) 2022/2555 of the European Parliament and of the Council concerning measures for a high common level of cybersecurity across the Union (NIS2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng. European Commission; *NIS2 Directive: securing network and information systems*. [2026]. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[13] ACER. *Cybersecurity network code for electricity*. Accessed 25 November 2026. https://acer.europa.eu/electricity/cybersecurity; Commission Delegated Regulation (EU) 2024/1366 supplementing Regulation (EU) 2019/943 as regards cybersecurity rules for cross-border electricity flows. 24 May 2024. https://eur-lex.europa.eu/eli/reg_del/2024/1366/oj/eng.

[14] World Economic Forum. *Risk Management, Reimagined: Outlook to 2035*. 18 September 2026. https://www.weforum.org/publications/risk-management-reimagined-outlook-to-2035.

[15] European Commission. *Guidelines on the application of Article 13(5) of Directive (EU) 2022/2557*. C/2026/3712; 13 July 2026. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026XC03712.

[16] DNV. *From Concern to Control: Rethinking Energy Resilience for the New Threat Era*. 25 August 2026, pp. 9–12. https://www.dnv.com/news/2026/from-concern-to-control-dnv-presents-resilience-framework-to-strengthen-critical-energy-infrastructure-as-threats-intensify/.

[17] CERT Polska. *Energy Sector Incident Report*. 30 January 2026. https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/.

[18] Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities (CER Directive), Articles 5–6; European Commission, High Representative of the Union for Foreign Affairs and Security Policy. *Strengthening EU economic security*. JOIN(2025) 977 final; 3 December 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0977; Regulation (EU) 2019/941 of the European Parliament and of the Council on risk-preparedness in the electricity sector. 5 June 2019 https://eur-lex.europa.eu/eli/reg/2019/941/oj/eng.; Regulation (EU) 2017/1938 of the European Parliament and of the Council concerning measures to safeguard the security of gas supply. 28 October 2017. https://eur-lex.europa.eu/eli/reg/2017/1938/oj/eng; Commission Delegated Regulation (EU) 2024/1366 supplementing Regulation (EU) 2019/943 as regards cybersecurity rules for cross-border electricity flows. 24 May 2024. https://eur-lex.europa.eu/eli/reg_del/2024/1366/oj/eng; ACER. *Cybersecurity network code for electricity*.

[19] Regulation (EU) 2019/941 of the European Parliament and of the Council on risk-preparedness in the electricity sector. 5 June 2019, Articles 6–10. https://eur-lex.europa.eu/eli/reg/2019/941/oj/eng; Commission Delegated Regulation (EU) 2024/1366 supplementing Regulation (EU) 2019/943 as regards cybersecurity rules for cross-border electricity flows. 24 May 2024. https://eur-lex.europa.eu/eli/reg_del/2024/1366/oj/eng. ACER. *Cybersecurity network code for electricity*.

[20] ENTSO-E. *Position Paper on the Security of Critical Infrastructure*. 31 August 2026, Recommendations 1–7. https://www.entsoe.eu/2026/08/31/entso-e-position-paper-on-the-security-of-critical-infrastructure/.

[21] For an industry-oriented framework for moving beyond compliance towards integrated and continuously tested resilience management, see DNV. *From Concern to Control: Rethinking Energy Resilience for the New Threat Era*. 25 August 2026, pp. 8–12. https://www.dnv.com/news/2026/from-concern-to-control-dnv-presents-resilience-framework-to-strengthen-critical-energy-infrastructure-as-threats-intensify/.

[22] Burilkov A, Pahon A, Ondrejkovičová DS. *Protecting Critical Infrastructure from Physical and Hybrid Threats*. GLOBSEC; 25 September 2026. https://globsec.org/what-we-do/publications/protecting-critical-infrastructure-physical-and-hybrid-threats.

[23] ENTSO-E. Position Paper on the Security of Critical Infrastructure. Recommendations 1–7.

[24] European Commission, High Representative of the Union for Foreign Affairs and Security Policy. *EU Preparedness Union Strategy*. 26 March 2025. https://commission.europa.eu/topics/preparedness_en.

[25] European Commission. *Submarine Cable Security Toolbox and Cable Projects of European Interest*. 5 February 2026. https://digital-strategy.ec.europa.eu/en/library/submarine-cable-security-toolbox-and-cable-projects-european-interest.

[26] Council of the European Union. *European grids package: Council backs modernised energy network for decarbonisation*. 26 June 2026. https://www.consilium.europa.eu/en/press/press-releases/2026/06/26/european-grids-package-council-backs-modernised-energy-network-for-decarbonisation/.

[27] McWilliams B, Tagliapietra S, Zachmann G. *Europe's energy information problem*. Bruegel Policy Brief 07/2025; 2025. https://www.bruegel.org/sites/default/files/2025-02/PB%2007%202025_0.pdf.

[28] European Parliament. *Strengthening energy security*. Legislative Train, 25 October 2026 update. https://www.europarl.europa.eu/legislative-train/package-security-of-energy-supply/file-strengthening-energy-security; EU-NATO Task Force. *Final Assessment Report on the Resilience of Critical Infrastructure*. June 2023. https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf. NATO. *NATO launches "Baltic Sentry" to increase critical infrastructure security*. 14 January 2025. https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security.

[29] Authors' adaptation from: DNV. *From Concern to Control*.

[30] Norwegian Ministry of Energy. *Sikkerhet og arbeidsmiljø i havindustriene*. 5 June 2026. https://www.regjeringen.no/no/dokumenter/sikkerhet-og-arbeidsmiljo-i-havindustriene/id3163854/.

[31] International Energy Agency. *Ukraine's Energy Security 2026: Pre-winter assessment 2026–2027*. 4 November 2026. https://www.iea.org/reports/ukraine-s-energy-security-2026.

[32] SANS Institute. *Confirmation of a Coordinated Attack on the Ukrainian Power Grid*. 6 January 2016. https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid.

[33] ESET. *Industroyer2: Industroyer reloaded*. 12 April 2022. https://blog.eset.ie/2022/04/12/industroyer2-industroyer-reloaded/.

NOTES

NOTES

The **European Policy Centre** is an independent, not-for-profit think tank dedicated to fostering European integration through analysis and debate, supporting and challenging European decision-makers at all levels to make informed decisions based on sound evidence and analysis, and providing a platform for engaging partners, stakeholders and citizens in EU policymaking and in the debate about the future of Europe.

The EPC's **Europe's Political Economy Programme** (EPE) focuses on EU economic governance, the single market, and digital, industrial, energy, trade, and economic security policies amid significant geo-economic and technological shifts. In a world of rising geopolitical competition and a fragmenting economy, the EPE has been at the forefront of research on Europe's competitiveness agenda, the "triple" green, digital and economic security transitions and 'wartime economy'. The EPE's cross-programme flagship initiative, the Brussels Economic Security Forum, examines EU-US-China dynamics, changing international economic rules and statecraft, as well as related EU policy challenges. As fast advancing components of economic security, critical emerging technologies in clean tech, the AI value chain and quantum are priority areas of focus. Using its convening power and multistakeholder taskforce model, the Programme aims to provide in-depth analysis and actionable recommendations to tackle key policy challenges. The EPE team comprises a diverse group of analysts with backgrounds from government, the private sector, academia, and journalism, bringing a broad range of expertise to its work.

With the strategic support of King Baudouin Foundation
Working together for a better society