Redesigning the EU's *Energy Security Architecture*

PAVING THE WAY TOWARDS A SECURE AND DECARBONISED FUTURE

Flaminia Bonanni, Luke O'Callaghan-White, Artur Patuleia

A central challenge of this decade will be ensuring the delivery of reliable and affordable energy for Europeans in the face of increasing and emerging security risks. As the EU transitions from a fossil fuel-based system to an increasingly renewable and electrified system, these physical, operational, cyber, geopolitical and economic risks will require a new energy security architecture that addresses cross-sectoral and evolving challenges.

In 2026, the EU has a key opportunity to update and future-proof this architecture. The European Commission's revision of the EU energy security framework, together with other legislation on the political agenda, offer the potential to embed a new and strategic approach to energy security: one that recognises and anticipates the security needs of an increasingly decarbonised and digital energy system.

Europe's vulnerability to fossil fuel imports has made the clean energy transition a strategic priority to deliver energy security. Across Europe, this transition from a fossil fuel system to a clean, renewable and electrified system has begun, accelerated by the security imperative. However, the existing energy infrastructure, risk assumptions, operational standards and solutions still reflect the realities of a fossil-based system, and not the security needs of the future energy system.

A redesign of the EU's energy security architecture is required to match the needs of this ongoing energy system transformation. With the review of the EU's energy security framework on the political agenda this year, the European Commission has a unique opportunity to embed the lessons from recent fossil crises and deliver the security benefits of the clean energy transition.

Ahead of this review, this briefing considers how Europe's energy system transformation and energy security needs intersect. As part of the analysis, it first sets out the security benefits of a renewables-based system – such as reduced exposure to geopolitical and global energy market instability, as well as improved system readiness and connectivity. This is followed by an assessment of five risk categories – physical, operational-planning, cyber, geopolitical and economic-financial – and the new or emerging threats within them.

While some risks are already well recognised, such as geopolitical and economic-financial, there are new or emerging risks that will require increased attention as the energy system transition progresses. Outdated operational standards for electricity networks, the development of new technology and adoption of AI, or the lack of investment in grid assets are among the threats which will need to be addressed to adapt to a new type of energy system.

To deliver a resilient energy system, EU and national policymakers must therefore prepare Europe's energy security architecture to anticipate and adapt to these evolving risk categories. This will require adopting a cross-sectoral and integrated approach that includes the following action:

- Combine the Security of Gas Supply Regulation and the Electricity Risk Preparedness Regulation to ensure an integrated approach to energy security.
- Introduce a 'security by design' principle into network planning to strengthen resilience against emerging security threats.
- Fully integrate climate resilience into energy security planning.
- Update system operation to match the needs of a high-renewables, electrified and digital system.
- Strengthen and upgrade cybersecurity requirements for energy infrastructure.
- Establish and secure competitive clean energy supply chains.
- Deliver the security benefits of cross border interconnection and regional system cooperation.

The case for a new energy security architecture

Europe is experiencing its second energy crisis in five years, and this has called into question the stability and reliability of the existing fossil fuel-based system. Instead, the transition away from fossil fuels and towards a clean energy future is increasingly recognised as a critical lever for delivering energy security. Yet the existing framework has not kept pace with the needs of this transition.

A new energy security framework is needed which can leverage the security benefits of a decarbonised energy system, while also recognising and addressing new challenges. The European Commission's revision of the energy security framework, expected in 2026, is critical: it offers the opportunity to review how the EU is anticipating, and responding to, evolving security risks as the energy system transitions to an integrated, decarbonised energy system. A successful update of the EU's security framework will take a cross-cutting and integrated approach: leveraging provisions from existing EU legislative files such as the Critical Raw Materials Act (CRM Act) and RESourceEU Action Plan, the Network and Information Security (NIS2) Directive and the Critical Entities Resilience (CER) Directive; as well as from legislation in progress, such as the European Grids Package and the Electrification Action Plan.

The EU has a critical opportunity to learn from the lessons of the recent energy shocks and geopolitical changes. Now is the moment to future-proof the EU's energy system by accelerating the transition to a renewables-based system while anticipating and preparing for the new and emerging risks.

Embed lessons from recent and ongoing fossil fuel crises

The EU pursued a strategy of gas import diversification following the 2022 Russian invasion of Ukraine. Given the EU's outsized dependence on Russia for its energy imports at the time, these measures were designed to provide short-to-medium-term stability for the energy system.

While the EU effectively and rapidly reduced Russian imports, it diversified its gas supplies, sourcing its liquefied natural gas (LNG) supplies from the United States and Qatar in particular.[1] Yet, this focus on diversification of fossil gas supply has not delivered lasting economic resilience, competitiveness nor energy affordability. Rather, it has created new dependences and geopolitical vulnerabilities. The weaknesses of this approach are evident in the context of the ongoing conflict in Iran, where the effective closure of the Strait of Hormuz has massively disrupted global fossil fuel supplies, leading to a surge in Europe's energy bill by the order of €60bn in the first 100 days of the conflict.[2]

[1] Eurostat, 2025, **Imports of liquefied natural gas by partner, 2025**

[2] Institut Jacques Delors, 2026, **War in Iran: 100 days in, €60 billion out**

Instead of seeking new fossil fuel contracts and pursuing alternative suppliers in response to the current crisis, EU policymakers should accelerate efforts to replace existing oil and fossil gas dependencies with clean alternatives.

The security benefits of the clean energy transition

The clean energy transition has and will continue to play an integral role in boosting European energy security. Achieving the full benefits of the transition (summarised in Table 1), requires the shift away from fossil fuel imports to go hand in hand with accelerated electrification, energy efficiency improvements and increased investment in, and planning of, future energy system needs.

Table 1. Security benefits of the clean energy transition

Change in the energy system	Security benefits
Harnessing Europe's abundant renewables capacity	▶ Reduce exposure of the energy system to geopolitical threats by replacing fossil fuel dependencies. ▶ Reallocate expenditures for fossil fuel imports into investments for domestic production and increased security standards.
Accelerating the uptake of electrification and energy efficiency	▶ Significantly reduce overall energy demand through energy efficiency improvements. ▶ Reduce exposure to global price volatility and market instability by increasing rate of renewable electricity.
Investing in grid infrastructure, demand flexibility and storage	▶ Improve system readiness in response to sudden disruption. ▶ Improve interconnection supporting power system stability. ▶ Deploy modern system features reducing demand peaks.

Harnessing Europe's abundant renewable capacity reduces collective dependence on fossil fuel imports and consequently mitigates exposure to international price spikes and market instability. In recent years, significant progress has been made. In 2025, EU wind and solar overtook fossil power generation for the first time;[3] the surges in wind and solar capacity between 2019 and 2025 resulted in €59 billion in avoided expenditure in fossil fuel imports for power generation;[4] and avoided approximately 92 billion cubic metres (bcm) of fossil gas imports.[5]

Together, increased electrification, accelerated energy efficiency and renewables deployment can structurally reduce energy needs while delivering on decarbonisation and resilience objectives. Operating such a system will require coordinated investment in infrastructure and upgraded capabilities, such as demand side flexibility, cross-border resource sharing and energy storage. These features will be needed to guarantee access to affordable energy, offer rapid restoration in the case of disruptions, and improve system stability.

Managing the energy transition: assessing the security risks

A clean energy system brings clear security benefits to the EU. However, this transformation is not a panacea and may itself pose energy security risks. A redesign of the EU's energy security architecture will need to account for both existing and new or emerging threats to energy system security as the EU transitions to a renewables-based system. This section provides an overview of these risks, which are summarised in Figure 1.

In this briefing, we use the term 'risk' to refer to an overarching category: physical, technical-operational, cyber, geopolitical and economic-financial. For each risk category, we analyse 'threats', by which we mean possible actions, events or conditions that could materialise to threaten energy security. For each threat we consider a core 'driving factor'. We also consider whether the given threat is '*new or emerging*' or '*existing*'. We define these terms as follows:

- **New or emerging**: a threat that is new or has emerged in recent years. We also consider threats as 'new' if the driving factor of the threat has recently emerged.
- **Existing**: a threat to energy security which is well established and widely recognised as such. 'Existing threats' could intensify without the sufficient mitigation measures.

[3] Ember, January 2026, **Wind and solar generated more power than fossil fuels in the EU for the first time in 2025**

[4] Ember, January 2025, **European Electricity Review 2025, Chapter 2.2. Green Deal cut the EU's fossil import bill**

[5] Ibid.

Assessment of security risks during the clean energy transition

RISK CATEGORY	THREAT	DRIVING FACTOR	EXISTING THREAT	NEW OR EMERGING THREAT
PHYSICAL	Military and hybrid threats	Conflicts and tensions among countries		X
	Extreme weather events	Change in frequency and intensity of extreme weather events	X	
OPERATIONAL PLANNING	Outdated system operation	Lack of grid flexibility or cross-border resources		X
	Misaligned grid planning and design	Inadequate system security and stability assumptions		X
CYBER	Cyberattacks	More frequent attacks on energy infrastructure	X	
	AI and smart enabled technologies	Automation and digitalisation of the energy system		X
GEO POLITICAL	Fossil fuel dependency	Geopolitical disruptions, chokepoints, weaponisation of assets	X	
	Critical raw materials	Access to materials and expected demand boost		X
ECONOMIC FINANCIAL	Energy cost rises	Role of gas as price setter	X	
	Misaligned infrastructure investment	Fossil infrastructure buildout misaligned with future demand	X	

Figure 1. E3G's assessment of risk categories and threats relating to the EU's energy system security in the transition to a renewables-based system.

Categorisation of risks

Physical risks

Military and hybrid threats

In recent years, hybrid attacks have caused significant damage to European energy assets.[6] Sabotage of energy infrastructure and damage to underwater pipelines have become a more frequent occurrence. This type of threat is among the most concerning due to the difficulties in detecting actual origin, confusion about the intended target and complications over legal responses and political coordination.

[6] Hybrid threats refer to coordinated harmful activities, carried out with malign intent to undermine a target, such as a state or an institution, through a variety of means, often combined. These means may include information manipulation, cyberattacks, economic influence or coercion, covert political manoeuvring, coercive diplomacy, or threats of military force. Hybrid tactics are used by both state and non-state actors. This definition comes from: **https://www.consilium.europa.eu/en/policies/hybrid-threats/**

Two European areas with a high level of exposure to hybrid risks are the Baltic Sea and the North Seas, both home to critical energy and telecoms infrastructure:

- Between February 2022 and late 2024, the Helsinki Commission reported a total of 150 hybrid Russian operations against NATO territory, 33% of which were critical Infrastructure attacks.[7]
- Between January 2022 and end of July 2025, 59 out of 89 successful Russian sabotage actions against Europe took place in the Baltic region, making it a new epicentre of hybrid threats.[8]

Experience from recent military attacks on energy infrastructure in Ukraine is instructive. Evidence on the ground shows that restoring fossil gas supplies is much more difficult than restoring disrupted electricity supply.[9] The near-total blackout in Ukraine in 2022 was restored with success due to the activation of operational network redundancies, deployment of decentralised backup equipment and rapid repair capabilities.[10] [11] By contrast, repairing gas compressor stations or pipeline surface sections often requires new construction of assets and specific equipment, making restoration of gas supply a more complex and longer process than addressing attacks on centralised electricity network infrastructure.[12]

Fossil installations are also inherently more vulnerable to a single point of failure due to centralised network infrastructure, while relying on less system flexibility overall.[13] The Russian attacks that took place at the end of 2025 on Ukrainian fossil gas infrastructure were already responsible for an estimated loss of up to 40–50% of daily gas production, significantly affecting winter preparedness. [14]

Extreme weather events

The increasing frequency and heightened intensity of extreme weather events pose a serious threat. Europe's energy infrastructure is increasingly exposed to more extreme conditions: from more frequent and intense heatwaves to changing precipitation patterns that can lead to catastrophic flooding or major rainfall declines followed by drought.[15]

---

[7] U.S. Helsinki Commission, December 2024**, Spotlight on the Shadow War: Inside Russia's Attacks on NATO Territory**

[8] Polish Institute of International Affairs (PISM), March 2026, **(Un)safe Waters: The Baltic Sea Region and the Redefinition of Security in Europe**

[9] Centre for Global Studies, July 2024, **Russian tactics targeting Ukrainian critical energy infrastructure**.

[10] Ibid.

[11] Dixi Group & International Renaissance Foundation, March 2026, **Holding the Grid: Ukraine's Energy Resilience Playbook**

[12] Centre for Global Studies, July 2024, **Russian tactics targeting Ukrainian critical energy infrastructure**.

[13] Ibid.

[14] Dixi Group & International Renaissance Foundation, March 2026, **Holding the Grid: Ukraine's Energy Resilience Playbook**.

[15] European Environmental Agency (EEA), 2024, **European Climate Risk Assessment**

These extremes not only pose physical risks to infrastructure, but also drastically change demand patterns, for instance increasing demand for cooling.

The flooding in western Europe during the summer of 2021 had a major impact on the region's energy infrastructure. In Germany, the fossil gas distribution network in the Ahr Valley was severely affected, with approximately 133 km of pipelines and over 7,000 household connections damaged or destroyed.[16] More recently, in January 2026, storm Kristin hit Portugal and caused more than 3,000 weather-related incidents and disrupted power supply to more than 850,000 people.[17]

The increasing demand for electrified solutions will require further attention to this type of threat. According to the IEA, power lines are among the most vulnerable assets, with damage to transmission and distribution grids accounting for 85% of incidents recorded globally in 2023.[18] In the same year, 210 million households globally experienced power cuts due to extreme weather events.[19] While Europe is among the continents with some of the most reliable and high-quality services,[20] the increasing frequency and intensity of such weather events will require additional measures to ensure system resilience.

Assessment

	RISK CATEGORY	THREAT	DRIVING FACTOR	EXISTING THREAT	NEW OR EMERGING THREAT
PHYSICAL		Military and hybrid threats	Conflicts and tensions among countries		X
		Extreme weather events	Change in frequency and intensity of extreme weather events	X	

[16] Koks, E. E. et al., 2022, **Brief communication: Critical infrastructure impacts of the 2021 mid-July western European flood event**, Nat. Hazards Earth Syst. Sci., vol. 22, 3831–3838.

[17] BBC, 28 January 2026, **At least five killed after Storm Kristin hits Portugal**

[18] International Energy Agency (IEA), 2025, **World Energy Outlook 2025**

[19] Ibid.

[20] Bruegel, Policy Brief Issue n˚31/24, December 2024, **Decarbonising for competitiveness: four ways to reduce European energy prices**

Operational-planning risks

Outdated system operation

Outdated operational standards pose a threat for systems that are rapidly electrifying and integrating high levels of renewables, but which continue to operate based on standards appropriate for a centralised fossil fuel-based system.

The EU investigation into the 2025 Iberian blackout concluded that Spain's system management failures were the main cause of the Peninsula's power system collapse.[21] These failures essentially resulted from outdated regulations and insufficient capabilities to support grid stability; this reduced the tools at the disposal of the Spanish system operator to manage grid disturbances in a context of a highly decarbonised and decentralised power system. Moreover, the blackout demonstrated the need for better coordination between system operations (across borders and between the national transmission and distribution network levels) to ensure visibility of real-time conditions and allow for rapid response from operators.

Delays in updating operational standards will also increase system vulnerability to rapidly changing demand patterns. The coming decade will likely see a rapid increase in electricity demand as new sources come online, altering traditional demand patterns. A system unable to respond to such changes with adequate demand flexibility will be at risk. This will put significant strain on system operation, particularly on grids with older, outdated infrastructure. Similarly, a lack of interconnection can reduce resilience of the overall system: the interconnections with France and Morocco were key to quickly powering up the grid in response to the 2025 blackout in Spain. But while a lack of interconnection can reduce resilience, increased interconnection also comes with threats that must be managed.

Misaligned grid planning and design

Lessons from the war in Ukraine clearly underscore the importance of embedding regional adequacy into network planning and design. Planning assumptions, including network investment decisions and technology procurement, must consider changing system needs to ensure redundancies and resilience are built into the system. This should consider both system adequacy (that is, the system's ability to meet demand) and resilience and operational preparedness against unexpected disturbances.

[21] The ICS Investigation Expert Panel consisted of a European Network of Transmission System Operators for Electricity (ENTSO-E) expert panel acting according to EU electricity market regulations – Regulation (EU) 2019/943 and Regulation (EU) 2017/1485; for its report see ENTSO-E, 20 March 2026, Grid Incident in Spain and Portugal on 28 April 2025

In an increasingly integrated European grid, local vulnerabilities may lead to widespread power supply consequences, reinforcing the need for regular security assessments as well as Europe-wide coordination and an alignment of security standards and operations.

Assessment

	RISK CATEGORY	THREAT	DRIVING FACTOR	EXISTING THREAT	NEW OR EMERGING THREAT
OPERATIONAL PLANNING		Outdated system operation	Lack of grid flexibility or cross-border resources		X
		Misaligned grid planning and design	Inadequate system security and stability assumptions		X

Cyber risks

Cyber-attacks

In 2023, the European Union Agency for Cybersecurity (ENISA) reported more than 200 cyber incidents targeting the energy sector.[22] Ransomware was the most common type of attack: exploiting digital vulnerabilities for financial gain through blackmail and targeted disruption of assets.[23] Survey data on changing attitudes and approaches to cybersecurity in the energy industry demonstrates that more than four in ten professionals (42%) believe cyber incidents will increase.[24]

There is a widening gap in cybersecurity standards between information technology (IT) and operational technology (OT) systems.[25] While IT cybersecurity is generally well developed, the more recent digitalisation of OT has not been matched by concurrent cyber protection.[26]

In particular, the lack of centralised coordination mechanisms is a concerning trend. For example, 32% of energy sector operations do not have a single critical OT process monitored by a Security Operations Centre (SOC).[27] This means that approximately one-third of energy infrastructure operates without real-time cyber surveillance, rendering existing security requirements and information frameworks unfit to address emerging sophisticated threats.

---

[22] ENISA, June 2024, **Cyber Europe tests the EU Cyber Preparedness in the Energy Sector**

[23] Ibid.

[24] NV CYBER, 2025, **Energy Cyber Priority 2025: Addressing evolving risk, enabling transformation**

[25] Operational technology refers to hard- and software that directly monitors and controls physical devices, processes and infrastructure in industrial settings

[26] ENISA, June 2024, **Cyber Europe tests the EU Cyber Preparedness in the Energy Sector**

[27] Ibid.

AI-enabled and smart technologies adoption

The aforementioned digital vulnerabilities could be exacerbated by the deployment of AI-enabled and smart technologies. Greater automation and digital integration can improve overall system functioning, by allowing more sophisticated grid response and reporting capabilities. However, it also adds a new layer of complexity to manage cyber risks. The increase of ransomware and data theft episodes identified by ENISA[28] becomes significantly more concerning, considering AI-enabled systems can generate and distribute data at speed and scale.

As the European energy system becomes more digitalised and increasingly embeds smart and AI-based tools, these new threats will only intensify. A renewables-based system, that is increasingly connected and decentralised, with higher-volume data exchanges, increases the number of possible entry points for cyber-attacks. In addition, greater interconnection across borders may increase exposure to the cascade effect[29] if not appropriately managed. Given the growing interconnection of the EU's power systems, a cyber-attack at a single vulnerable point could thus have far-reaching and cross-border impacts, making the case for strong EU-level coordination of OT as well as IT cyber security an imperative.

Assessment

	RISK CATEGORY	THREAT	DRIVING FACTOR	EXISTING THREAT	NEW OR EMERGING THREAT
CYBER		Cyber-attacks	More frequent attacks on energy infrastructure	X	
		AI and smart enabled technologies	Automation and digitalisation of the energy system		X

Geopolitical risks

Fossil fuel dependency

An energy system heavily reliant on fossil fuel imports is vulnerable to global political and economic instability, chokepoint disruptions and the weaponisation of energy assets. The EU's dependency on fossil fuel imports keeps the bloc exposed to these vulnerabilities with implications for socioeconomic stability.

The EU has repeatedly found itself facing the geopolitical implications of this dependence. The war in Ukraine is one such example, with Russia using gas supplies to exert pressure

[28] ENISA, 2024, **ENISA threat landscape 2024 – July 2023 to June 2024**

[29] A cascade effect is an unforeseen chain of events that occurs when an event in a system has a negative impact on other, related systems.

on the EU.[30] In urgently seeking alternative gas supplies, the EU had to accept less favourable contracting terms with other state actors, as illustrated by the EU–Qatar LNG supply agreement.[31] The pivot away from Russian pipeline imports also turned the United States into the EU's most significant LNG supplier, accounting for around 56% of these imports, making US LNG deliveries a central element in recent EU–US trade negotiations.[32] Moreover, Russia continues to supply nearly 14% of the EU's LNG and is the EU's second largest supplier of LNG.[33]

The 2026 energy crisis, resulting from the conflict in Iran and closure of the Strait of Hormuz, has demonstrated that regardless of suppliers, fossil fuel dependence remains a structural threat due to the volatile nature of these markets and the ease with which systemic vulnerabilities can propagate.[34]

Critical raw materials

In the shift to a renewables-based electrified energy system, the access to, and supply of, critical raw materials (CRMs) can be considered an emerging threat. Concentrated dependence on few suppliers or possible disruptions to supply chains must be managed, especially given the highly concentrated nature of extraction, mining and processing, which currently takes place in just a few countries. In addition, the significant demand growth expected in the coming years – for instance a nine-fold increase in lithium demand by 2040[35] – coupled with increased competition for these supplies, will put pressure on supply chains. These risks may be mitigated by improving circularity approaches to recover and re-use already imported stocks while design innovation can improve material use.

A new energy security approach should understand and assess the differences in the energy security risk profiles of fossil fuels and CRMs. Fossil fuel systems rely on a continuous flow of fuel supplies, creating persistent security risks and leading to immediate consequences if disrupted. Conversely, renewables depend on clean supply chains, consisting mostly of equipment and CRMs, which can be stockpiled or recovered and, once installed, provide long-term energy, not being subject to the same short-term storage and transit vulnerabilities.[36] Moreover, storage of CRMs faces far fewer technical challenges than the long-term storage of fossil fuels, such as fossil gas.

---

[30] European Commission, 2023, New reports highlight 3rd quarter impact of gas supply cuts

[31] Bloomberg, June 2022, **Qatar to Demand EU Sign Long-Term LNG Deals If It Wants More Gas**

[32] European Commission, 2025, **EU-US trade deal explained - energy aspects**

[33] Eurostat, 2025, **Imports of liquefied natural gas by partner, 2025**

[34] The geopolitical vulnerabilities of continued dependence on fossil oil and gas imports due to disruptions of chokepoints is explored in depth in the E3G report, March 2026, **Beyond Securing Supply, Chokepoint risk for oil and gas importers**

[35]European Commission, Raw Materials Information System (RMIS) **Future Demand for Raw Materials in Emerging Technologies – A Global Perspective** – **https://rmis.jrc.ec.europa.eu/** - accessed May 2026

[36] E3G, March 2026, **Beyond Securing Supply, Chokepoint risk for oil and gas importers**

Assessment

	RISK CATEGORY	THREAT	DRIVING FACTOR	EXISTING THREAT	NEW OR EMERGING THREAT
GEO POLITICAL		Fossil fuel dependency	Geopolitical disruptions, chokepoints, weaponisation of assets	X	
		Critical raw materials	Access to materials and expected demand boost		X

Economic and financial risks

Energy prices

During the EU's 2021–2023 energy crisis, monthly average gas prices on the TTF stood at over 130 EUR/MWh,[37] more than seven times higher than the average between 2016 and 2021.[38] Due to the role of gas as marginal price-setter, EU wholesale electricity prices spiked sharply as well, ranging between 150 and 300 EUR/MWh during the same year.[39]

The electricity bills of European consumers remain exposed to sudden price increases as long as fossil gas continues to set the price of electricity. Increasing the share of renewable energy and displacing fossil gas in the power system through storage, flexibility and operational upgrades would support greater wholesale price stability and contribute to more stable and predictable electricity prices for consumers.

In the EU, there are differences among Member States when it comes to the degree of renewable integration and dependence on fossil gas for power systems. These differences have important impacts on electricity bills. For example, during the first ten days of the recent blockade of the Strait of Hormuz, fossil gas set the electricity price for just 15% of the hours in Spain's high-renewables system, compared with 60% of the hours in Germany and 90% in Italy.[40] In the first quarter of 2026, electricity prices in Spain were 56% lower than in Germany and 65% lower than in Italy.[41]

[37] TTF stands for Title Transfer Facility – a Durch virtual trading point which is currently Europe's biggest gas benchmark

[38] ACER & CEER, October 2023, **European gas market trends and price drivers**

[39] ACER, February 2023, **Wholesale Electricity Market Monitoring 2022**

[40] Ember, March 2026, **Latest energy shock reminds Europe of its risky gas reliance**

[41] Fraunhofer Institute for Solar Energy Systems (ISE) Energy-Charts: quarterly electricity spot market prices, **https://energy-charts.info/charts/price_average/chart.htm?l=en&c=DE&interval=quarter&quarter=1** and **https://energy-charts.info/charts/price_average/chart.htm?l=en&c=IT&interval=quarter&quarter=1**

Misaligned infrastructure investment

The fossil gas supply shortage experienced during the EU's 2021–2023 energy crisis led to significant investment in Europe's LNG regasification capacity, which increased by 13% in 2023 and 8% in 2024, and is expected to further increase in 2026.[42]

However, this infrastructure buildout is misaligned with the trajectory of European energy demand. Demand for LNG is anticipated to decrease by about 23% by 2030.[43] This is investment in infrastructure that will not be needed in the coming decades, adding to a stock of stranded assets which must eventually be dealt with and decommissioned. This is in fact already the case for some investments made during the 2021–2023 energy crisis. For example, in October 2025, TotalEnergies announced the decommissioning of a fossil gas terminal due to lack of activity over the previous two years.[44]

Conversely, European electricity demand is expected to reach over 50% of final energy consumption by 2050.[45] Enabling this demand will require significant amounts of capital: nearly €1.2 trillion in electricity grid investments by 2040.[46] The mismatch between capital allocation and infrastructure needs therefore presents a significant hurdle as Europe moves forward with the clean energy transition.

Assessment

	RISK CATEGORY	THREAT	DRIVING FACTOR	EXISTING THREAT	NEW OR EMERGING THREAT
ECONOMIC FINANCIAL		Energy cost rises	Role of gas as price setter	X	
		Misaligned infrastructure investment	Fossil infrastructure buildout misaligned with future demand	X	

[42] Institute for Energy Economics and Financial Analysis (IEEFA) European LNG Tracker, **https://ieefa.org/european-lng-tracker**, last updated May 2026

[43] Ibid.

[44] InfluenceMap, 15 December 2025, **Industry Voices Challenge the Pro-Fossil Gas Narrative on EU Energy Security**

[45] European Commission, 2024, Impact Assessment accompanying the report: **Securing our future Europe's 2040 climate target and path to climate neutrality by 2050 building a sustainable, just and prosperous society**

[46] European Commission: Directorate-General for Energy, Trinomics, Artelys, LBST, Finesso, A. et al., **Investment needs of European energy infrastructure to enable a decarbonised economy – Final report**, Publications Office of the European Union, 2025

Delivering a secure energy system: Recommendations for lasting European energy security

Building a new energy security architecture that delivers a resilient energy system and captures the security benefits of the energy transition will require anticipating and adapting to these different risk categories. The changing and evolving nature of the frequency and intensity of these risks, as outlined in the previous section, will require an adaptive and agile approach.

Some of these risks are already well understood, such as damages caused by extreme weather events to physical infrastructure, or the impact of fossil import dependence on energy price volatility. Other risks have emerged more recently. These include system vulnerability from a lack of demand side flexibility and cross border interconnection, the development of new technology and adoption of AI, and the geopolitical dimension to supply of critical raw materials. Furthermore, some risks are interlinked. For instance, geopolitical instability could increase exposure to hybrid attacks while outdated operational standards could leave the system unable to recover in case of disruption.

EU and national policymakers have an opportunity to embed a new strategic approach to energy security both during the revision of the energy security framework and across other legislative files.[47]

The following section outlines recommendations that EU and national policymakers should adopt to strengthen Europe's energy security architecture by tackling the existing and emerging risk profiles, outlined above.

Recommendations

Combine the Security of Gas Supply Regulation and the Electricity Risk Preparedness Regulation to ensure an integrated approach to energy security

The EU's energy security legislation is underpinned by two regulations: the Security of Gas Supply Regulation[48] and the Electricity Risk Preparedness Regulation[49]. These regulations provide rules for Member States to apply in emergency settings. In 2026, the European

[47] For instance, the NIS2 Directive, the Critical Raw Materials Act, the RESourceEU Action Plan, the Electrification Action Plan and the European Grids Package.

[48] Official Journal of the European Union, **Regulation (EU) 2017/1938 concerning measures to safeguard the security of gas supply**

[49] Official Journal of the European Union, **Regulation (EU) 2019/941 on risk-preparedness in the electricity sector**

Commission will propose updates to these pieces of legislation as part of the energy security framework revision. The Commission should:

- Introduce a single overarching regulation that covers both gas and electricity. Combining the two existing regulations would avoid duplication and favour the adoption of coordinated solutions for an increasingly integrated European energy system. An overarching regulation would also allow for a single Coordination Group, comprising relevant stakeholders, to support the identification of common solutions in a changing system, which would enhance energy security governance at the EU level.

Introduce a 'security by design' principle into network planning to strengthen resilience against emerging security threats

Integrating security needs into an early stage of infrastructure planning and system design can improve system preparedness. Several pieces of EU legislation, including the energy security framework Revision, but also the European Grids Package and the Electrification Action Plan, present an opportunity to harmonise and embed the principle of 'security by design'. This includes:

- Adapting assumptions that underpin system engineering and design, and procurement and tender criteria to consider the latest security risk assessments. This may be further complemented by the application of enhanced protection, detection and repair capabilities to energy infrastructure development as well as streamlined information exchange among Member States. It should also include ensuring continuous updates and regular security assessments are applied to system restoration protocols and data.
- Feeding the results from national and cross border security assessments, including joint exercises, into system recovery playbooks as well as update processes for network design and operation. These assessments should reflect new or emerging risks and should be coordinated with defence stakeholders. The results could be integrated into the Central Scenario process proposed by the European Grids Package to address vulnerabilities to the European grid, especially in the context of cross-border projects.

Fully integrate climate resilience into energy security planning

The increasing frequency and intensity of extreme weather events will require both physical infrastructure and system operation to adapt. Improved grid redundancies and new engineering and design approaches will increase the reliability of electricity supply during extreme events and reduce outage times. This should include:

- Reassessing existing grid design and operation approaches, electricity supply restoration capabilities, and the role of decentralised operation to prepare for identified climatic changes and improve seasonal and weather-related preparedness.

The European Climate Resilience and Risk Management – Integrated Framework[50] can serve as a guide for mapping climate risks to security requirements.

Update system operation to match the needs of a high-renewables, electrified and digital system

The features traditionally supporting system resilience in a fossil-fuel energy system are not appropriate for an increasingly electrified, digital and renewables-based system. The rapid changes in the energy system require not only timely implementation of updated network standards, but also the deployment of electronic-based assets able to provide grid stability services. This will require:

- Updating system operation protocols in areas like voltage control, network integration of renewable energy generators, rules for dispatch and disconnection and monitoring and coordination between TSO and DSOs. System restoration capabilities, grid stability and flexibility capacities should be regularly assessed for adequacy against the operational reality of a high renewables, electrified and digital power system.
- Planning system infrastructure with future system needs in mind, including consideration of new assets and services supporting grid stability like storage, electronics-based grid services providers and demand side flexibility. Forward-looking, integrated and independent infrastructure planning can help avoid misalignment of investment and better ensure delivering a cost-effective system.

Strengthen and upgrade cybersecurity requirements for energy infrastructure

As cyber and AI-related tools become increasingly used to manage and operate energy infrastructure, the system needs strengthened protection against cyber threats. The benefits of overall improved system functioning and real-time responsiveness that increasingly digital systems offer, could be offset by increased risk if cybersecurity standards do not keep pace. This is particularly relevant as Europe develops a more interconnected system across countries. This will require:

- Developing EU-level guidance that sets out cyber-energy security requirements to address the intersection of energy and cyber legislation and enable harmonised implementation across the EU.
- Aligning cyber security standards across Member States to further improve emergency response capabilities to cyber-attacks. This will entail additional risk management measures and increased cross-border cooperation, information sharing, supervision and enforcement of the NIS2 Directive.

[50] **European Climate Resilience and Risk Management – Integrated Framework**, accessed June 2026

Establish and secure clean energy supply chains

Stable and predictable supply chains for critical clean technologies will be crucial for securing Europe's clean energy transition. Given the particularly concentrated nature of CRM extraction, mining and processing and the anticipated surge in demand for CRMs as well as other cleantech components, clean energy supply chain management will become a critical political issue as the EU continues transitioning towards a renewables-based and electrified energy system. Existing EU legislation can help make the most of existing stockpiles and accelerate developing circular approaches to CRMs and clean technologies. For example, the CRM Act sets benchmarks by 2030 for domestic capacity with at least 25% of the EU's annual consumption for recycling.[51] Policymakers should take further action to:

- Promote secondary use of materials, recycling and long-term planning on resource use. Strategic stockpiling of CRMs is also essential but must happen alongside increased materials circularity and optimised design of clean technologies.
- Coordinate supply chain development regionally and at European level to build domestic manufacturing and production capacities while strengthening visibility and predictability.

Deliver the security benefits of cross border interconnection and regional system cooperation

A more interconnected European energy system can mitigate system disruptions, provide additional sources for stable network operation and deliver speedy system restoration in emergencies. However, delivery of cross-border projects is still hampered by political, economic and financial barriers, as this infrastructure is primarily assessed based on its contribution to market integration and economic benefits. The security benefits of interconnectors should be more prominently assessed as part of the investment decision-making process. Stronger regional cooperation can contribute to enhanced preparedness in the event of system disruptions and should be streamlined and leveraged. These benefits can be delivered by:

- Recognising the critical role of interconnectors for Europe's energy security. The EU's energy security framework must recognise the enabling role of interconnectors in sharing resources for cross-border grid stability support and in restoring electricity supply after a system outage.
- Strengthening regional cooperation frameworks to enhance repair and system restoration capabilities, including equipment and operational teams, and coordinate on the implementation of investments and regulations that improve cross-border system stability.

[51] **Critical Raw Materials Act - Internal Market, Industry, Entrepreneurship and SMEs**, accessed May 2026

ABOUT E3G

E3G is an independent think tank working to deliver a safe climate for all.

We drive systemic action on climate by identifying barriers and constructing coalitions to advance the solutions needed. We create spaces for honest dialogue, and help guide governments, businesses and the public on how to deliver change at the pace the planet demands.

More information is available at **www.e3g.org**

COPYRIGHT

AUTHORS

Flaminia Bonanni is a Senior Researcher within the EU energy transition team at E3G. Her work focuses on EU's energy system transformation and buildings decarbonisation.

Luke O'Callaghan-White is Programme Lead for EU energy transition at E3G.

Artur Patuleia is a Senior Policy Advisor at E3G. His work focuses on the EU's energy system transition and on the resilience and security of energy infrastructure.

ACKNOWLEDGEMENTS

We are grateful to all the EU energy security experts who engaged with earlier versions of this briefing over recent months. Within E3G, we wish to thank all those who reviewed draft versions, and in particular Chiara Celesia and Rheanna Johnston for their rich contributions to the research and analysis of this briefing. which has strengthened the final output. For their diligent work in copy editing this briefing, we are grateful to E3G's Daniele Gibney and to Dr Kathrin Luddecke.