cerre Centre on Regulation in Europe

CYBER RESILIENCE AS A PILLAR OF EUROPEAN ENERGY SECURITY

ISSUE PAPER

December 2025

Alessandro Lazari

As provided for in CERRE's bylaws and procedural rules from its “Transparency & Independence Policy”, all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this report has been prepared, received the support and/or input of the following CERRE member organisations: Bayernwerk, E.ON, GRDF, Ofgem, PPC, Terna, and Utility Regulator Northern Ireland. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or of members of CERRE.

info@cerre.eu – www.cerre.eu

Executive Summary

Europe's energy system is undergoing a profound transformation driven by decarbonisation, decentralisation, and digitalisation. While these changes enhance efficiency and sustainability, they also expose the energy sector to an increasingly complex risk landscape shaped by cyber threats, climate extreme events, geopolitical tensions, supply chain dependencies, and hybrid campaigns. In this context, cyber resilience is no longer a purely technical issue but a structural pillar of energy security, market stability, industrial safety, and public trust.

The paper argues that traditional, siloed approaches to security – separating cyber, physical, climate, and market risks – are no longer fit for purpose. Modern energy systems function as deeply interconnected socio-technical ecosystems in which cascading failures can rapidly propagate across borders and sectors. Hybrid threats, combining cyber intrusions, physical sabotage, economic coercion, and disinformation, further amplify systemic vulnerability, particularly in lifeline infrastructures such as electricity and gas.

From a technological perspective, the rapid deployment of distributed energy resources (DERs), IT/OT convergence, legacy operational technologies, and cloud-based industrial platforms has dramatically expanded the cyber-attack surface. At the same time, globalised and opaque supply chains, vendor lock-in, and proprietary digital ecosystems undermine trustworthiness and limit operators' capacity to verify or rapidly replace insecure components. Emerging threats – such as ransomware, AI-driven attacks, data integrity manipulation, and cloud concentration risks – compound these challenges.

The paper maps the evolving EU regulatory framework relevant to energy cyber resilience, including the Network and Information Security Directive (NIS2), the Critical Entities Resilience (CER) Directive, the Cybersecurity Act (CSA), the Cyber Resilience Act (CRA), the Seveso III Directive, and the Network Code on Cybersecurity (NCCS). Collectively, these instruments significantly strengthen Europe's resilience posture by addressing cybersecurity risk management, all-hazards resilience, product security, supply chain transparency, and cross-border operational coordination. In particular, the CRA represents a structural shift by making secure-by-design, vulnerability handling, and lifecycle security legally enforceable for digital products used in energy systems.

However, the analysis identifies persistent governance, technical, and systemic gaps. These include:

- Incomplete regulatory coverage of DERs and prosumer-level technologies;
- Fragmented supervision across cyber, safety, civil protection, and energy authorities;
- Weak integration between cybersecurity, climate adaptation, and industrial safety;
- The absence of energy-specific cybersecurity technical standards and certification schemes;
- Ongoing risks related to vendor lock-in, supply chain opacity, and dependence on foreign high-risk suppliers;
- Limited consideration of space-based dependencies – including Global Navigation Satellite System (GNSS), satellite communications, Earth observation – in energy resilience planning.

To address these gaps, the paper proposes a three-level strategic roadmap:

1. Regulatory consolidation in the short term: Prioritise full, harmonised implementation of NIS2, CER, and CRA across Member States before introducing new legislative layers.

2. Creation of a European Programme for Critical Entities Resilience (EPCER): A renewed operational platform to support cross-sector exercises, stress testing, best-practice exchange, and hybrid threat preparedness.

3. Long-term structural evolution: Introduce a "DORA-like" regime – similar to the EU's Digital Operational Resilience Act (DORA) – for lifeline infrastructures, starting with energy, to impose stronger vendor oversight, audit rights, substitution strategies, and supervision of systemic digital service providers.

In parallel, the paper calls for sector-specific cybersecurity certification for energy digital components, to be developed by the European Union Agency for Cybersecurity (ENISA) under the Cybersecurity Act, and for enhanced EU guidance on integrating cyber, physical, climate, and hybrid risks into unified resilience assessments.

Overall, the paper concludes that embedding cyber resilience into EU energy regulation requires a shift from compliance-driven security to a systemic, anticipatory, and strategically integrated resilience model, capable of sustaining Europe's energy systems under compound shocks and long-term geopolitical pressure.

This paper is part of the CERRE's Forum series "*Towards an Integrated Approach to Infrastructure and Market Resilience*", which includes two papers that have already been published: on the revision of the EU's security of supply framework in the context of growing electrification and decarbonisation[1], and on the integration of climate resilience into regulation[2]. Upcoming papers will further explore resilience in supply chains, market-related supply disruptions, and the review of the energy security framework.

[1] Banet, C., & Le Coq, C. (2025). *Updating the Security of Energy Supply Architecture and Preparedness Toolbox for an Increasingly Electrified Energy System*. Centre on Regulation in Europe (CERRE).
[2] Baldursson, F. M., & von der Fehr, N.-H. M. (2025). *Embedding Climate Resilience in Regulation*. Centre on Regulation in Europe (CERRE).

Table of Contents

1. Introduction

Europe's energy system is undergoing a profound transformation. Decarbonisation, decentralisation, and digitalisation are reshaping the architecture of electricity and gas markets, creating a more interconnected, data-driven, and highly automated ecosystem. While these developments support climate objectives and efficiency gains, they also expose the energy sector to an increasingly complex and interdependent risk landscape. Cybersecurity threats, extreme weather events, supply chain disruptions, geopolitical tensions, and hybrid threat campaigns challenge the foundations of the EU's energy regulation. In such an environment, embedding cyber resilience into energy regulation is no longer optional; it is a structural requirement for ensuring the confidentiality, integrity, availability[3] (C-I-A) and trustworthiness of energy systems across the European Union. Seen through this mapping, cyber resilience is no longer a purely digital concern but becomes a structural enabler of energy security, market stability, industrial safety, and public trust. This reinforces the need to embed cybersecurity explicitly within the regulatory architecture governing energy resilience, also ensuring that principles are operationalised across both cyber and physical dimensions.

1.1 The Shifting Risk Landscape in Europe

Recent assessments of risks in Europe underline a decisive shift: hazards are no longer isolated or linear, but systemic, cascading, cross-border, and hybrid in nature. The "*Analysis of Risks Europe Is Facing* " published by the Joint Research Centre (JRC) identifies 47 distinct risks across natural, technological, geopolitical, societal, and cyber domains, emphasising that Europe's exposure stems from the interactions between these risks, not merely from their individual presence[4]. These risks amplify one another through complex feedback loops: a climate-induced extreme event can overstretch critical infrastructures, which in turn increases vulnerability to malign cyber activity; geopolitical confrontation can combine with economic pressure to destabilise energy supplies, while disinformation campaigns erode public trust in institutions and aggravate political polarisation.

For the energy sector, given its role as a lifeline vital service, this environment is particularly sensitive because it sits at the intersection of physical networks, cyber-physical control systems, market mechanisms, and geopolitically exposed supply chains. According to ENISA's *Threat Landscape 2025*,

[3] From a cybersecurity perspective, resilience is traditionally articulated through the triad of Confidentiality, Integrity, and Availability (C-I-A). When translated into the regulatory and operational language of the energy sector, this model provides a powerful analytical bridge between digital security and energy system resilience. Confidentiality, in the energy context, is not limited to the protection of sensitive data. It directly underpins market integrity, operational security, and national security, as energy trading platforms, dispatch systems, and grid monitoring infrastructures rely on protected information flows. Breaches of confidentiality may enable market manipulation, targeted sabotage, or strategic intelligence extraction affecting critical infrastructure. Integrity maps onto the trustworthiness of physical and cyber-physical operations. The integrity of measurements, control signals, protection relay settings, and automated balancing mechanisms is fundamental to grid stability and industrial safety. A loss of integrity – through data manipulation, firmware tampering, or insider interference – can trigger cascading technical failures, including Seveso-type accident scenarios in gas storage and LNG facilities. Availability directly corresponds to the traditional concept of security of supply and service continuity. Denial-of-service attacks, ransomware incidents, cloud service outages, or satellite-based timing disruptions translate immediately into reduced operational availability of generation, transmission, and distribution assets, with systemic economic and societal consequences.

[4] European Commission, Joint Research Centre, *Analysis of Risks Europe Is Facing*, 2025, pp. 18–24.

energy is consistently among the most targeted sectors for sophisticated cyber operations[5]. The report stresses three dynamics that heighten systemic vulnerability:

- the professionalisation and industrialisation of ransomware groups and other threat actors;
- supply chain compromises that penetrate energy systems via software and hardware dependencies;
- exploitation of digital interdependencies, including cloud-based industrial control systems and remote management interfaces.

These dynamics operate simultaneously with climate and environmental risks, which the JRC identifies as among the most impactful and fastest-growing categories of risk for Europe[6]. Heatwaves, droughts, wildfires, and severe storms increasingly impact energy production, transmission, and distribution. Hydropower output, gas cooling systems, and nuclear power plant safety margins all face growing strain. At the same time, high-impact, low-probability events – such as geomagnetic storms or large-scale technological failures – pose additional systemic hazards and threats.

The risk landscape is also shaped by geopolitical shocks, including armed conflict, economic coercion, and deliberate targeting of energy infrastructures. Europe's experience following the Russian invasion of Ukraine illustrates the exposure of energy markets to geopolitical pressure, market manipulation, and supply disruption. These shocks combine with disinformation campaigns aimed at influencing public perceptions of energy policy or destabilising democratic debate.

A further critical dimension concerns the growing dependency of the European energy system on foreign suppliers of digitally enabled equipment. Much of this equipment is developed, manufactured, and maintained outside the European Union, often within complex and opaque global value chains. This dependency generates a dual risk profile. From a geopolitical perspective, it raises issues of strategic autonomy, exposure to coercive economic practices, and potential disruption of access to spare parts, updates, and technical support during geopolitical crises. From a cybersecurity perspective, it amplifies the risk that vulnerabilities, malicious code, backdoors, or insecure update mechanisms may be embedded at the design or manufacturing stage.

In essence, Europe's risk environment is multifaceted, dynamic, and hybrid – and cyber threats are deeply intertwined in this broader context.

1.2 The Evolving Notion of Resilience

Originally, resilience in the energy sector referred primarily to technical reliability: the ability to provide uninterrupted service despite equipment failures, peak loads, or localised disruptions. Over time, this narrow concept expanded to include physical protection, operational continuity, and emergency preparedness. Nowadays, resilience must be understood as a systemic, anticipatory, and multidimensional capability that integrates cyber, physical, climate, market, societal, and geopolitical dimensions.

[5] ENISA, *Threat Landscape 2025*.
[6] European Commission, Joint Research Centre, *Analysis of Risks Europe Is Facing*, 2025, sections 3.1.2.4 and 3.1.2.5.

Given these premises, three conceptual evolutions[7] are pivotal for embedding cyber resilience in energy regulation:

A shift from single-hazard to multi-hazard thinking

Risks rarely manifest in isolation. Cyberattacks may coincide with adverse weather conditions; a grid operator may face simultaneous operational, logistical, and communication disruptions[8]. Therefore, energy systems require an integrated approach to resilience that anticipates compound shocks and cascading failures.

The rise of hybrid threats

The JRC's work on hybrid threats demonstrates how state and non-state actors deploy multi-domain, coordinated campaigns that combine cyber intrusions, economic pressure, disinformation, supply chain interference, and – in some cases – direct or indirect physical sabotage[9]. These campaigns exploit systemic vulnerabilities rather than isolated weaknesses. For energy systems, this means that cyber resilience must coexist with:

- **economic resilience**, to withstand market manipulation or coercive pricing;
- **informational resilience**, to address disinformation targeting energy operators, regulators, and citizens;
- **supply chain resilience**, to secure access to critical and trustworthy technologies, components, and materials (continuity of supply and C-I-A of supply);
- **societal resilience**, because public trust affects policy implementation, emergency responses, and investment decisions.

A move towards anticipatory governance

Foresight analysis by ENISA indicates that future cyber threats will be shaped by rapid AI-enabled automation, quantum-capable adversaries, and a proliferation of insecure connected devices[10].

[7] The evolution from asset-centric security towards systemic resilience is now explicitly embedded in public policy narratives and corporate strategies. At European level, recent policy communications on energy security, climate adaptation, digital sovereignty, and critical entities resilience increasingly frame resilience as a cross-sector, multi-domain capability, rather than as a purely technical or sectoral attribute.

[8] The systemic interdependence between energy and digital infrastructures has been repeatedly demonstrated in real-world incidents. Severe weather events have shown that power outages cascade almost immediately into disruptions of telecommunications, data centres, and emergency communications, while, conversely, failures in telecom networks can severely impair grid monitoring and restoration operations. During Storm Boris (Central Europe, 2023), widespread electricity outages caused the temporary collapse of mobile and fixed communications in several regions, delaying grid situational awareness, emergency coordination, and customer notification.

[9] Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/37899, JRC129019.

[10] ENISA, *Foresight Cybersecurity Threats for 2030 – Update.*

Therefore, anticipatory regulation[11] needs to look beyond compliance with minimum standards and instead cultivate adaptive capacity, redundancy, and learning mechanisms within the energy sector.

Taken together, these evolutions suggest that energy regulation should embrace a holistic (or system as a whole [12]) resilience paradigm where cyber resilience is both a distinct field of action and a foundational requirement for all other dimensions of resilience. In this perspective, resilience also becomes a core dimension of economic security and, ultimately, of European strategic autonomy, as the ability to protect and sustain the functioning of energy systems underpins industrial competitiveness, societal stability, and geopolitical independence.

1.3 Risks to the Energy Market in a Systemic Environment

The risk landscape facing the European energy sector can be grouped into four broad but interrelated clusters: cybersecurity threats, climate and environmental risks, geopolitical and economic risks, and societal and informational risks.

Cybersecurity threats

Derived from ENISA's analyses, the most often recurring cyber risks for the energy sector include:

- ransomware targeting operational technology;
- disruptive attacks on industrial control systems;
- supply chain compromise, particularly through software updates and embedded components;
- advanced persistent threats seeking pre-positioning within grid operator networks;
- "living-off-the-land" attacks exploiting legitimate processes in energy management systems.

These attacks increasingly exploit the expansion of distributed energy resources, digital substations, and cloud-connected monitoring platforms.

Climate and environmental risks[13]

[11] Anticipatory regulation refers to a forward-looking regulatory approach that seeks to identify, prepare for, and shape emerging risks and technologies before they fully materialise, rather than reacting ex post through corrective compliance mechanisms. This concept has been extensively developed in European regulatory studies, among those "Toward Anticipatory Regulation and Beyond" by Georg Serentschy, Paul Timmers, and Marja Matinmikko-Blue as appears in "The Changing World of Mobile Communications", 2023, Palgrave Macmillan Cham.

[12] "System as a whole" within the resilience paradigm refers to the capacity of an interconnected socio-technical system to withstand, absorb, adapt to and recover from disruptive events across multiple domains simultaneously. In the energy sector, this includes not only individual physical assets or digital components, but also interdependencies between generation, transmission, distribution, digital control systems, markets, supply chains, telecommunications, space-based services and societal trust. System as a whole resilience therefore exceeds the sum of individual asset protections and requires coordinated governance across sectors, borders and risk domains.

[13] For a detailed account of climate-related regulatory challenges and resilience measures, see: Baldursson, F. M., & von der Fehr, N.–H. M. (2025). *Embedding Climate Resilience in Regulation*. Centre on Regulation in Europe (CERRE).

The JRC identifies heatwaves, droughts, wildfires, and floods as among the most frequent and impactful risks for Europe's energy systems. Impacts include reduced generation efficiency, compromised cooling systems, physical damage to transmission infrastructure, and heightened volatility in electricity wholesale markets.

Geopolitical and economic risks

Europe faces persistent geopolitical tensions, including attacks on undersea cables and pipelines, coercive energy trade practices, and hybrid campaigns targeting critical infrastructure. Market turbulences – such as the 2021-2023 energy price crisis – introduces additional destabilisation risks for consumers and operators[14].

Societal and informational risks

Disinformation and information manipulation campaigns targeting energy policy can erode public support for emergency measures or infrastructure projects. Misinformation can lead to behavioural shifts that complicate demand management, while reputational attacks on energy companies may affect crisis communication and regulatory trust[15].

These clusters are not isolated; they form an entangled network of risks where one shock can amplify another. A cyberattack on a grid operator during a heatwave, or a coordinated disinformation campaign launched during an energy supply crisis, can produce systemic effects well beyond the initial event[16].

1.4 Towards a Comprehensive Understanding of Risk in Energy Regulation

Given the converging pressures described above, energy regulation must evolve from a narrow focus on technical performance and security of supply to a whole-system resilience approach. This means recognising that:

[14] Recent years provide multiple examples of geopolitically driven supply chain and infrastructure disruptions affecting Europe's economic and energy security. These include the sabotage of undersea infrastructure in the Baltic Sea and geo-economic interventions in strategic industrial assets. High-profile cases in the broader digital-industrial ecosystem (e.g. state scrutiny over foreign acquisitions of semiconductor firms) illustrate the growing intersection between cybersecurity, supply chain security and economic sovereignty. The 2021–2023 energy price crisis further demonstrated how geopolitical shocks can rapidly translate into systemic economic stress.

[15] A relevant example is the Trans Adriatic Pipeline (TAP) landing site in Melendugno (Lecce, Italy), where infrastructure works were repeatedly obstructed during the construction phase due to strong local opposition fuelled by misinformation regarding environmental and health risks. The polarisation of public opinion, amplified through social media and activist networks, led to violent protests, sabotage attempts, and attacks on construction sites. This case illustrates how disinformation and perceived risk narratives can directly translate into physical threats to critical energy infrastructure and delay strategic projects of European interest.

[16] A paradigmatic example of systemic cascading effects is the Colonial Pipeline ransomware attack in May 2021, which disrupted fuel supplies across the U.S. East Coast, triggered panic buying, caused fuel shortages at filling stations in several states, and forced emergency interventions. The incident demonstrated how a single cyberattack on an energy operator can rapidly propagate into transportation, logistics, emergency services, and social domains. Comparable cascading dynamics could be expected in Europe during concurrent stress conditions such as extreme heatwaves, geopolitical or supply chain crises (e.g. the 2021 Suez Canal obstruction).

- Cyber resilience is essential to protect the digital “nervous system” of the energy sector;
- Physical resilience is needed to withstand climate-induced stresses;
- Market resilience is required to absorb price volatility and supply shocks;
- Societal and informational resilience safeguards trust and behavioural stability;
- Hybrid threat awareness is needed to anticipate coordinated, cross-domain disruption;
- Supply chain resilience underpins technological sovereignty[17] and operational continuity.

This systemic perspective should not replace sector-specific approaches; rather it should constitute criteria and thresholds along which modern frameworks should be aligned to be better suited to an era of interconnected risks.

[17] At EU level, technological sovereignty is pursued through a broad policy ecosystem that goes beyond cybersecurity regulation. In addition to the Cyber Resilience Act (CRA) and the Cybersecurity Act (CSA), this includes the EU Industrial Strategy, the Critical Raw Materials Act, the Net-Zero Industry Act, and the Chips Act for semiconductor independence. Together, these instruments aim to reduce excessive dependencies on third-country suppliers and strengthen trusted value chains for digital and energy technologies.

2. Rethinking Resilience: Integrating Cyber, Physical, Climate, Market, and Hybrid Dimensions

For decades, resilience in the energy sector was equated with technical reliability: the capacity of assets to withstand mechanical failure, extreme temperatures, or overload conditions. Regulatory frameworks were designed around the stability of supply, protection of critical nodes, and emergency preparedness within well-defined sectoral boundaries. This model implicitly assumed that risks were largely local, predictable, and bounded by the infrastructure itself.

However, as digitalisation, climate change, globalisation of supply chains, and geopolitical volatility reshape the energy sector, the notion of resilience has evolved. The emergence of cross-sector and cross-border risks has revealed that energy systems cannot be safeguarded through asset-centric approaches alone. Instead, resilience must be understood as a systemic property, shaped by interactions between physical assets, cyber-physical systems, market mechanisms, social behaviours, and geopolitical forces[18].

This shift from asset-centric protection to systemic resilience has profound implications for corporate governance, operational procedures, cross-sector cooperation, and the design of regulatory frameworks, which are synthesised in

Table 1 below.

Table 1: From a traditional approach to systemic resilience.

Dimension	Asset-Centric Security (Traditional Approach)	Systemic Resilience (Emerging Paradigm)
Object of protection	Individual assets	Entire socio-technical energy system
Corporate governance	Cybersecurity and physical security as technical functions	Resilience integrated into risk management and strategic planning
Risk assessment	Single-hazard and site-specific risk analysis	Multi-hazard, cross-domain and cascading risk analysis (cyber, climate, hybrid, market)
Operational procedures	Separate cyber, safety, and continuity plans	Integrated cyber-physical-climate continuity and crisis management

[18] European Commission, Joint Research Centre, *Analysis of Risks Europe Is Facing*, 2025.

Dimension	Asset-Centric Security (Traditional Approach)	Systemic Resilience (Emerging Paradigm)
Supply chain management	Focus on cost, performance, and contractual reliability and liabilities	Strategic focus on trustworthiness, diversification, transparency, and geopolitical risk
Inter-operator cooperation	Limited to sector-specific operational coordination	Structured cross-sector cooperation (energy, telecoms, transport, cloud)
Regulatory oversight	Siloed supervision	Coordinated multi-authority supervision and shared situational awareness
Crisis management	Incident response within a single domain	Multi-domain crisis response
Resilience objective	Prevent failure of individual components	Preserve continuity and recovery of the entire system under compound shocks

Source: elaborated by the author.

This shift from isolated, sector-specific resilience to systemic resilience represents one of the most significant conceptual evolutions affecting energy regulation today.

2.1 Interdependencies and Cascading Failures

The modern energy system is structured around deeply interconnected layers. Electricity networks rely on ICT infrastructure for real-time control; gas transmission depends on compressor stations powered by electricity; renewable integration requires advanced automation and forecasting tools; and market functioning depends on data availability, trust, and transparency. These interdependencies mean that disruptions, even if relatively small at the source, can cascade across systems and borders.

Recent JRC analysis illustrates that the majority of Europe's risks produce cascading effects[19] rather than isolated impacts, particularly when digital, physical, and environmental stressors coincide.

The energy system, therefore, increasingly operates under conditions where partial failures can scale into systemic ones, especially when operators, regulators, and Member States do not share a unified situational awareness.

[19] Evidence of cascading and compound impacts can be found in multiple European crises: (i) the 2025 large-scale blackout in Spain triggered by a combination of extreme weather, grid instability and operational constraints, which disrupted transport, digital services and emergency response; (ii) the earthquakes in Emilia-Romagna (2012) and Amatrice (2016), where physical destruction of energy and telecom infrastructure severely affected industrial production, healthcare and public communications; and (iii) the recurrent wildfires in Greece, which simultaneously damaged electricity networks, disrupted telecommunications and forced large-scale population evacuations.

2.2 Hybrid Threats as a New Layer of Systemic Risk

As described by JRC, hybrid campaigns combine cyber intrusions, physical sabotage, economic coercion, disinformation, and supply chain interference into coordinated strategies designed to exploit systemic vulnerabilities. Hybrid threats target dependency structures: cross-border pipelines, digital industrial control systems, maritime choke points, satellite communication links, and public trust itself.

In the energy domain, hybrid threat activity may include:

- cyber operations against SCADA or energy market platforms;
- interference with GPS and satellite-based timing systems used for grid synchronisation;
- pressure on LNG supply routes through maritime harassment or diplomatic coercion;
- disinformation aimed at undermining public acceptance of infrastructure projects or emergency measures;
- targeted manipulation of spare parts supply chains.

Therefore, hybrid threats reinforce the need for resilience strategies that look beyond the technical perimeter of individual assets or operators[20].

2.3 Why Siloed Approaches Fall Short: The Case for Systemic Resilience

The following concrete examples demonstrate the limits of siloed resilience thinking and the necessity of systemic approaches.

2.3.1 Gas Transmission and Critical Underwater Infrastructure

Much recent attention has rightly focused on the vulnerability of critical underwater gas infrastructure, including offshore pipelines and subsea interconnectors. High-profile sabotage incidents have elevated awareness of underwater segments as potential points of failure.

However, a fixation on subsea infrastructure alone obscures the fact that gas delivery depends on an entire chain of assets and actors. Each link operates in distinct jurisdictions, under different regulatory regimes, and with varying levels of threat and hazard exposure.

The European Union's energy system remains structurally dependent on gas imported through regions in which hybrid threat activity, political instability, or insufficient regulatory oversight may undermine

[20] Hybrid threat activity typically combines cyber, physical, economic and information tools to generate cascading systemic effects. Among the documented cases, the Nord Stream pipelines sabotage (2022) stands out as a hybrid operation combining physical infrastructure attack and geopolitical coercion, with direct consequences for European energy security and markets.

the continuity of supply. As a result, gas expected through a transcontinental pipeline somewhere in Europe may never arrive – simply because someone, thousands of kilometres away, did not secure an extraction facility, protect a compressor station, monitor a maritime bottleneck, or guard against hybrid pressure in a politically fragile corridor.

This simple observation exposes a fundamental truth: targeting a single infrastructure layer without assessing the resilience of the entire system produces a false sense of security.

2.3.2 LNG Maritime Dependencies and Strategic Choke Points

Europe's growing reliance on LNG increases its exposure to geopolitical risks affecting maritime routes. Key LNG flows transit through chokepoints routinely affected by geopolitical tension, piracy, physical incidents, and hybrid interference[21].

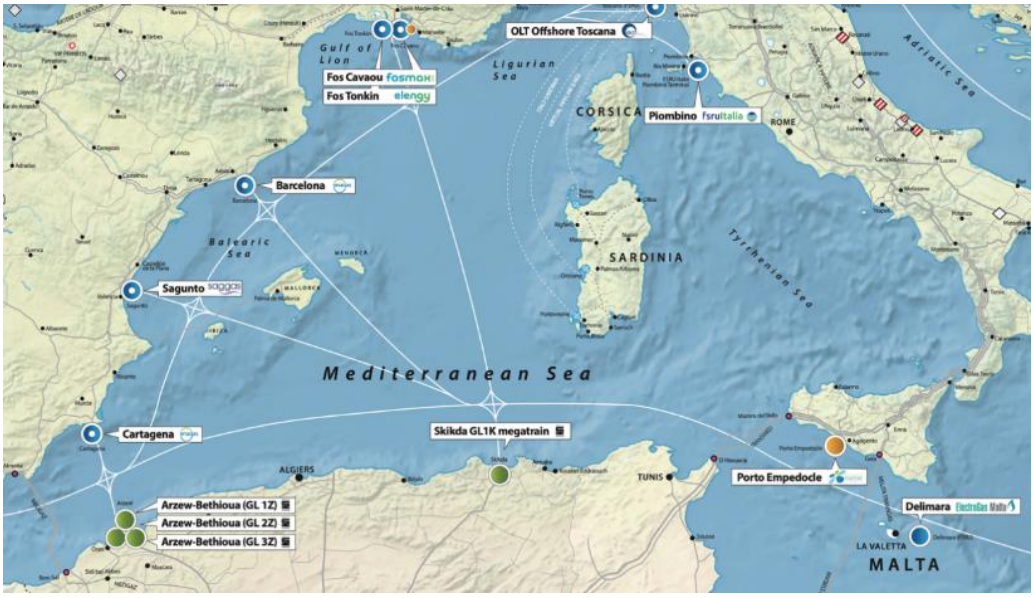

Figure 1: Portion of the GIE LNG map

Source: Gas Infrastructure Europe[22].

A localised security incident at any of these points may produce far-reaching consequences for European gas markets.

[21] Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/37899, JRC129019.

[22] Available at the following link: https://www.gie.eu/publications/maps/gie-lng-map/ Website visited on the 28th of November 2025.

2.3.3 Space-Based Telecommunications: An Overlooked Dependence

Energy systems increasingly rely on satellite-based services: GNSS for grid synchronisation, satellite telecommunications for remote substations, and space-based Earth observation for forecasting demand and renewable generation (and also monitoring wildfires and seismic activities).

Regulatory and resilience efforts, however, tend to focus on the ground segments, such as satellite control centres, terrestrial uplinks, or antenna arrays. The space-based segments – satellites, orbital infrastructures, spectrum vulnerabilities, debris risks, and cyber intrusions targeting spacecraft – often remain insufficiently addressed[23].

This asymmetry represents a critical blind spot on which energy operators should gain situational and operational awareness.

2.4 Implications for Energy Regulation

The examples above allow the formulation of the following conclusions: siloed approaches to resilience are incompatible with the operational reality of modern energy systems.

For energy regulation, this implies three core needs:

Integrated risk assessment and governance

Regulation must promote cross-sector and cross-border coordination, ensuring that cyber resilience assessments account for dependencies on physical infrastructure, ICT providers, maritime routes, space systems, and the geopolitical landscape.

Multi-domain situational awareness

Regulators and operators require mechanisms to understand how disruptions in one domain may propagate into others. This includes incorporating hybrid threat intelligence, foresight methodologies, and systemic stress-testing into regulatory oversight.

Incentives for whole-of-system resilience

[23] Extreme space weather, for example, represents a major but often under-addressed systemic risk for space-based infrastructures and the terrestrial services that depend on them. According to Joint Research Centre analysis, geomagnetic storms, solar flares and radiation storms can simultaneously disrupt satellites, GNSS positioning, satellite communications, aviation, rail signalling and high-voltage power transmission grids, with cascading cross-border effects capable of overwhelming national response capacities. Historical events (e.g. the 1989 Québec blackout and the 2003 Halloween storms) demonstrated transformer damage, satellite anomalies, aviation rerouting and widespread communication failures. The JRC highlights persistent knowledge gaps in impact modelling, limited early-warning lead times, hidden GNSS dependencies embedded in critical systems, and the growing vulnerability introduced by increasing digital interdependencies between space and ground infrastructures. These dynamics confirm that satellites must be treated as integral components of European critical infrastructure protection and resilience policy, rather than as peripheral or even ancillary technical domains. A detailed analysis is available in: Krausmann, E., Andersson, E., Gibbs, M. and Murtagh, W., Space weather and Critical Infrastructures: Findings and Outlook, EUR 28237 EN, Publications Office of the European Union, Luxembourg, 2016, ISBN 978-92-79-63903-6, JRC104231.

Operators should be encouraged to invest not only in asset-specific security but also in upstream and downstream resilience, supply chain transparency, cross-border cooperation, and crisis communication capacity.

3. Cyber Threats and Vulnerabilities in the Evolving Energy System

Energy system digital transformation – including distributed energy resources, smart devices, automated substations, remote monitoring, cloud-based analytics, and AI-enabled optimisation tools – is becoming ubiquitous across the energy value chains. These technologies introduce a diverse and expanding cyber-attack surface. This chapter examines the main categories of cyber vulnerabilities. It also touches on the importance of trustworthy systems, the risks of vendor lock-in, and proposes an early rationale for exploring dedicated cybersecurity certification mechanisms for digital components used in energy infrastructures.

3.1 Distributed Energy Resources (DERs) and Smart Inverters

The rapid growth of distributed energy resources has created a highly decentralised and heterogeneous landscape. These assets increasingly rely on smart inverters, IoT-based controllers, mobile applications, and cloud-integrated services to support two-way power flows, demand response, and local balancing.

From a cybersecurity perspective, the primary risks include:

- Highly dispersed attack surface: individual devices are geographically distributed, often installed in unmonitored environments, and connected through consumer networks;
- Weak default configurations: many devices retain default usernames, passwords, or authentication settings, and are shipped with outdated firmware or insecure communication protocols;
- Internet-exposed management interfaces: researchers have repeatedly found remotely accessible DER controllers, sometimes without authentication or with outdated encryption;
- Insecure interoperability: DERs communicate across vendor-specific protocols, often lacking robust security controls.

The SolarWinds compromise of 2020, though not energy-specific, demonstrated how a single compromised update can infiltrate thousands of organisations simultaneously – an attack pattern that could be replicated in grid management software, inverter firmware, or digital substation components.

A similar systemic logic underpinned the NotPetya malware attack of 2017, which exploited a software vulnerability and caused billions of euros in losses across critical sectors, including severe disruptions to energy companies' operations and logistics in several European countries.

DERs, therefore, boost grid resilience but create vast cyberattack surfaces, impacting system stability through vulnerabilities in connected devices (solar, wind, EVs, storage) and control networks. Since many DER operators are households, small businesses, or prosumers that fall outside the categories of "essential" or "important" entities under the NIS2 Directive, as well as inverter manufacturers and

aggregators, this means that they may not be explicitly considered critical operators despite their systemic importance.

3.2 Legacy Systems and IT/OT Convergence

Large parts of Europe's critical energy infrastructure rely on legacy operational technology (OT) designed decades ago without modern cybersecurity features. Many systems still use:

- outdated operating systems that cannot be patched;
- gateways with limited security controls;
- unencrypted industrial protocols;
- older protection relays or programmable logic controllers (PLCs) with minimal authentication.

The convergence of IT and OT has intensified these vulnerabilities. As operators integrate analytics platforms, remote monitoring, enterprise resource systems, and cloud-based dashboards, pathways are created that allow intrusions originating in IT networks to pivot into OT environments.

3.3 Supply Chain and Vendor Vulnerabilities

Energy operators depend on a global supply chain of hardware and software[24] which makes modern energy systems exposed to supply chain cybersecurity risks, including:

- compromised software updates, which may introduce malicious code;
- infected firmware or hardware implants, potentially pre-positioned during manufacturing;
- vulnerabilities inherited from third-party libraries integrated into industrial products;
- supply chain coercion, where state-linked actors influence vendors or logistics routes;
- product end-of-life support, because of obsolescence or cessation of operation (including bankruptcy) of the vendor.

Geopolitical concerns further complicate supply chains, as some vendors may be headquartered in jurisdictions with adversarial strategic interests or weak cybersecurity governance. Standards in other jurisdictions have acknowledged this reality: the North American NERC CIP standards include explicit supply chain risk management provisions, requiring utilities to assess vendor practices, update processes, and remote access pathways[25]. The NIS2 Directive similarly mandates supply chain scrutiny and identifies supplier security as a core requirement for essential and important entities[26].

Finally, supply chain vulnerabilities tie directly to trustworthiness and vendor lock-in. Many energy technologies are proprietary, integrated, and controlled through closed ecosystems. Operators may become dependent on a single vendor for patches, updates, diagnostic tools, or integration interfaces.

[24] E.g. SCADA systems, remote terminal units, protection relays, industrial sensors, communication gateways, grid management platforms, mobile applications, and cloud services.
[25] NERC CIP-013 standard on supply chain risk management in the North American bulk electric system. Available at the following link: https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-013-2.pdf
[26] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).

When vulnerabilities emerge, the operator may have limited ability to replace components, diversify suppliers, or independently validate security claims. This situation strengthens the case for transparent, trusted, and verifiable assurance mechanisms, including the exploration of the **possibility of a dedicated certification scheme within the meaning of the EU Cybersecurity Act**[27].

3.4 Emerging Threat Vectors

Beyond the core vulnerabilities described above, several emerging threats further complicate the cybersecurity landscape:

- Ransomware and Extortion Campaigns: Actors increasingly target energy companies with ransomware, exploiting weak remote access pathways or stolen credentials. The Colonial Pipeline incident illustrated how even intrusions in IT networks can lead to large-scale service disruption.
- Insider Threats: Both malicious and unintentional insiders can cause significant harm through misconfigurations, misuse of privileged accounts, or negligent handling of sensitive information.
- AI-Driven Attacks: As operators integrate machine-learning systems for forecasting, optimisation, and anomaly detection, attackers may attempt to poison training data, manipulate models, or deceive automated systems.
- Data Integrity Attacks: The manipulation of market data, sensor readings, or operational logs could undermine grid stability, market transparency, and situational awareness.
- Cloud Dependency Risks: Increased reliance on cloud-based industrial platforms creates centralised points of failure and shifts trust to third parties whose own security controls may vary.

These vectors underscore the need for cybersecurity approaches that account for complex interdependencies, cross-sector exposures, and system-wide impacts.

3.5 From Vulnerabilities to Regulatory Imperatives: The Role of Trustworthy Systems

The vulnerabilities identified above converge to highlight a central regulatory concern: energy systems rely on digital components whose security cannot be assumed but must be assured.

The ERNCIP[28] feasibility studies on Industrial Automation and Control Systems (2016-2020) repeatedly emphasised that trust cannot be established through technical claims alone; it requires structured

[27] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act).
[28] European Reference Network for Critical Infrastructure Protection. Flagship project of the European Programme for Critical Infrastructure Protection (2008 – 2020).

assurance, transparent testing, and verifiable conformity assessment[29]. Vendor lock-in, insecure supply chains, and legacy technologies amplify this need.

This need is even more acute today as the rapid diffusion of Industrial Internet of Things (IIoT) and Operational Technology (OT) connectivity has dramatically expanded the attack surface of energy systems, while the current EU certification landscape still lacks dedicated schemes for these high-impact environments. The Commission itself has explicitly identified Industrial Automation and Control Systems (IACS) and IoT as priority areas for future European cybersecurity certification, precisely due to their systemic relevance and persistent exposure to supply-chain and lifecycle vulnerabilities[30].

While the Cybersecurity Act has created a horizontal framework for European cybersecurity certification, the evidence from JRC and ERNCIP studies, as well as the Union Rolling Work Programme for Cybersecurity Certification (2024), suggests that general certification is often insufficient for the operational, safety-critical, and systemic characteristics of energy systems. **These studies constitute the initial rationale – without yet developing the full proposal – for exploring sector-specific certification approaches for digital components used in energy infrastructures.**

[29] European Commission, JRC (2015). Industrial Automation & Control Systems Cybersecurity: Introduction to the ICCS Framework (ERNCIP IACS TG). JRC102550. European Commission, Joint Research Centre (JRC) Theron, P. and Lazari, A. (2018). The IACS Cybersecurity Certification Framework (ICCF): Lessons from the 2017 Study of the State of the Art. EUR 29237 EN. Luxembourg: Publications Office of the European Union. ISBN 978-92-79-85968-7. doi:10.2760/856808. JRC111611. European Commission, Joint Research Centre (JRC) (2020). Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS). JRC121520.

[30] "*Union Rolling Work Programme for European cybersecurity certification*". SWD(2024) 38 final. European Commission.

4. Mapping the Regulatory Landscape for Energy Cyber Resilience

The European Union has developed an extensive regulatory architecture to strengthen the resilience of its energy systems. This architecture comprises horizontal cybersecurity legislation, sector-specific resilience obligations, industrial safety requirements, and emerging initiatives in cybersecurity certification. While these instruments collectively advance cyber resilience, their interaction remains complex, especially given the increasing convergence of cyber, physical, climate, and hybrid threats.

4.1 The Network and Information Security 2 (NIS2) Directive

The NIS2 Directive is the European Union's primary horizontal instrument for cybersecurity risk management. It replaces the original 2016 NIS Directive and significantly expands its scope and obligations. Energy system actors classified as "essential entities" include electricity and gas transmission system operators (TSOs), distribution system operators (DSOs), LNG terminals, gas storage facilities, hydrogen operators, and major power generation facilities.

Key Provisions Relevant to Energy Cyber Resilience

NIS2 mandates the implementation of comprehensive cybersecurity risk management measures, including:

- incident prevention, detection, response, and crisis communication;
- supply chain and supplier security assessments, including evaluation of vendor practices;
- multi-factor authentication, secure configurations, and vulnerability management;
- obligations for incident reporting within strict timeframes;
- oversight through audits, inspections, and sanctions by national competent authorities.

NIS2 also reinforces executive accountability, requiring management bodies to oversee cybersecurity implementation and potentially incur liability for failures.

4.2 The Critical Entities Resilience (CER) Directive

The CER Directive[31] introduces a comprehensive, all-hazards framework for the resilience of critical infrastructure across eleven sectors, including electricity, gas, oil, and hydrogen. Unlike NIS2, which focuses on cybersecurity, CER adopts a systemic view that encompasses **physical security**, organisational measures, operational continuity, and cross-border dependencies.

Expanded Threat Landscape under CER

[31] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive).

A defining feature of the CER Directive is its explicit acknowledgement that threats to critical infrastructure arise from multiple sources:

- severe weather events;
- climate change impacts;
- geopolitical tensions;
- hybrid threats;
- terrorist attacks.

CER thus recognises that physical security is not secondary to cybersecurity, but an integral component of resilience.

Implications for Energy Operators

Energy infrastructure is particularly exposed to climate-driven and hybrid threats. For example, transmission lines are vulnerable to extreme temperatures; LNG terminals and gas storage facilities may face increased storm risks; cross-border pipelines may be exposed to geopolitical instability or sabotage. CER's emphasis on cross-border dependencies is directly relevant, as many energy supply chains extend through jurisdictions with different threat landscapes. In this way, CER complements NIS2 and informs the systemic perspective required to achieve cyber resilience in energy systems.

4.3 The Cybersecurity Act (CSA)

The Cybersecurity Act establishes the European cybersecurity certification framework and strengthens ENISA's mandate. It aims to increase trust in products, services, and processes, recognising that security-by-design and transparency are essential for critical sectors such as energy.

Relevance to Energy Systems

The CSA enables the creation of European cybersecurity certification schemes. These schemes are voluntary unless made mandatory through secondary legislation. For the energy sector, certification is particularly relevant – yet not limited – to the following areas:

- industrial control systems;
- protection relays and digital substations;
- smart meters and advanced metering infrastructure;
- remote terminal units and communication gateways;
- IoT sensors, DER controllers, and supervisory platforms.

While existing EU certification schemes are horizontal, preparatory analyses by the JRC and the ERNCIP highlight the importance and feasibility of certification for industrial systems. Many energy technologies involve long operational lifecycles, proprietary interfaces, and system-wide interdependencies, which **require assurance mechanisms adapted to energy's specific risk profile**.

4.4 The Cyber Resilience Act (CRA)

The Cyber Resilience Act (CRA)[32] broadens the scope of cybersecurity obligations by placing mandatory requirements on manufacturers of hardware and software products with digital elements. It applies across sectors and introduces obligations for:

- vulnerability handling processes;
- security-by-design and secure default configurations;
- conformity assessment and CE marking for digital products;
- incident reporting for exploited vulnerabilities;
- obligations extending across the entire product lifecycle.

Significance for Energy Cyber Resilience

The CRA represents a structural shift in how cybersecurity is embedded into products with digital elements across the European Union, with direct implications for the energy sector. Cybersecurity becomes legally enforceable across the entire lifecycle of digital components, from design and manufacturing to deployment, maintenance, and decommissioning. This horizontal approach is particularly significant for energy systems, where digital components are deeply embedded in generation assets, substations, pipelines, LNG terminals, smart grids, and distributed energy resources.

The CRA introduces binding secure-by-design and secure-by-default obligations for manufacturers. Energy-relevant products are now required to be engineered with systematic risk assessment, attack surface minimisation, and protection against known exploitation techniques. For grid operators and energy infrastructure managers, this establishes a new baseline of technical assurance that was previously left to voluntary standards or procurement clauses.

Strict lifecycle vulnerability management duties are also imposed, including coordinated vulnerability disclosure, mandatory security updates, and defined support periods. This is particularly relevant for energy infrastructures where equipment lifecycles span 15–40 years, yet software vulnerabilities evolve on a scale of days/months.

The CRA strengthens supply chain transparency and software dependency control, notably through requirements related to due diligence on third-party components and the increasing use of software bills of materials (SBOMs). Energy infrastructures are among the most supply-chain-dependent systems in Europe, relying on globally sourced hardware, firmware, embedded operating systems, cloud interfaces, and remote maintenance platforms. By making manufacturers legally responsible for assessing and controlling inherited vulnerabilities, the CRA helps mitigate systemic exposure to opaque third-party software risks – an issue repeatedly demonstrated by major supply chain compromises.

[32] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act).

Differentiated conformity assessment regimes are also introduced for important and critical products with digital elements, including the possibility of mandatory European cybersecurity certification. A substantial subset of energy-related digital components falls naturally within the CRA's definition of products whose compromise may generate large-scale cascading effects across essential services. This creates the legal basis for sector-specific application of high-assurance certification schemes in the future.

Technical cybersecurity risks are also connected with non-technical strategic risks, including economic security and dependency on high-risk foreign suppliers. By recognising geopolitical exposure, jurisdictional risks, and state-influenced supply chains as legitimate cybersecurity factors, the CRA aligns cyber resilience with the broader agenda of European strategic autonomy. For the energy sector, this linkage is fundamental. It confirms that cyber resilience is not only a defensive technical property but also an instrument of economic security and sovereignty.

Finally, the CRA reinforces the integration between product security and operational resilience frameworks such as NIS2 and sectoral critical infrastructure regulation. Products certified and maintained under CRA requirements directly support compliance with risk management, incident prevention, and supply chain security obligations imposed on energy operators. This introduces a vertically coherent regulatory chain between manufacturers, integrators, operators, and regulators.

A summary of the domains covered by the CRA is provided in the

Table 2 below.

Table 2: CRA Domains and their significance for Energy Cyber Resilience.

CRA Domain	Core Requirement	Significance for Energy Systems
1. Secure-by-Design & Risk-Based Development	Products must be designed and developed with cybersecurity risks addressed from the outset.	Shifts energy OT, grid devices, and digital substations away from "bolt-on security" toward intrinsic resilience.
2. Vulnerability Handling & Lifecycle Management	Mandatory processes for vulnerability discovery, disclosure, patching, and coordinated remediation.	Directly addresses patching delays in energy OT environments and improves resilience against exploit persistence.
3. Secure Supply Chain & Third-Party Components (SBOM & Due Diligence)	Manufacturers must manage third-party risks and maintain software bills of materials (SBOMs).	Enables energy operators to assess embedded digital risk in digital components, strengthening cyber supply chain transparency.
4. Secure Update & End-of-Support Obligations	Security updates must be provided for defined support periods and installed securely.	Reduces systemic vulnerability caused by unsupported firmware in long-lived energy assets.

CRA Domain	Core Requirement	Significance for Energy Systems
5. Conformity Assessment & CE Marking	Products must demonstrate compliance through proportionate conformity assessment procedures.	Introduces market-level cyber assurance for energy digital components, reinforcing procurement security and reducing exposure to insecure equipment, including imported ones.
6. High-Risk & Critical Products with Mandatory Certification	Certain categories may be subject to mandatory European cybersecurity certification.	Opens the regulatory pathway for future sector-specific mandatory certification of critical energy digital components.

Source: elaborated by the author.

4.5 The Seveso III Directive

The Seveso III Directive[33] governs the control of major-accident hazards involving dangerous substances. It applies to a broad range of industrial facilities that are integral to Europe's energy value chain.

Relevance for Cyber and Physical Resilience

Seveso III establishes obligations for operators to:

- identify major-accident hazards;
- develop safety management systems;
- conduct risk assessments;
- implement preventive and mitigation measures;
- ensure emergency preparedness and public information.

Seveso III intersects with cyber resilience in two important ways. First, cyber incidents can trigger or exacerbate major-accident scenarios. Second, Seveso installations are increasingly digitalised and interconnected with energy networks. Integrating Seveso III requirements with NIS2 and CER is essential to avoid fragmented approaches across facilities that play a critical role in gas storage, LNG regasification, and petrochemical supply chains. **This alignment remains an emerging area of regulatory coordination.**

4.6 System Security Measures and Network Codes

The 2024 Commission Delegated Regulation establishing a network code on sector-specific cybersecurity rules for cross-border electricity flows represents the most concrete operationalisation to date of cybersecurity obligations within the EU electricity market framework. It introduces binding,

[33] Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances (Seveso III Directive).

sector-specific cybersecurity requirements for entities whose operations affect cross-border electricity flows, thereby translating the horizontal principles of NIS2 into actionable energy system governance.

The Regulation applies to entities identified as high-impact or critical-impact for cross-border electricity flows, including:

- Transmission and distribution system operators (TSOs and DSOs);
- Market operators and NEMOs;
- Regional coordination centres;
- Critical ICT service providers supporting electricity system operations.

The obligations are not triggered by sector classification alone but by the impact of an entity's digitalised business processes on cross-border electricity flows. This represents a significant conceptual shift from traditional asset-based regulation towards functional and systemic cybersecurity governance.

A major regulatory innovation concerns cyber-enabled electricity crisis management. The Regulation:

- Establishes a common definition of a simultaneous electricity crisis with a cybersecurity root cause;
- Introduces coordinated prevention, preparedness, and response mechanisms;
- Aligns electricity crisis management with:
    - the 2025 EU Cyber blueprint;
    - EU-CyCLONe under NIS2;
    - the EU Integrated Political Crisis Response (IPCR) arrangements.

This creates, for the first time in electricity regulation, a formal bridge between energy crisis management and EU-level cyber crisis coordination structures. Cyber incidents affecting electricity are therefore no longer treated as purely technical disruptions but as potential politico-strategic security incidents.

Strategic Relevance for Energy Cyber Resilience

From a systemic resilience perspective, the Regulation marks three strategic advances:

- Cybersecurity is elevated to a core parameter of electricity system security, on par with frequency stability, adequacy, and operational safety.
- Cross-border cyber risk becomes a shared European regulatory concern, not a purely national supervisory issue.
- Supply-chain cybersecurity, incident coordination, and operational testing are fully internalised within electricity governance.

4.7 Interaction, Complementarities, and Gaps

Taken together, NIS2, CER, the Cybersecurity Act, the Cyber Resilience Act, Seveso III, and network codes form a comprehensive – yet complex – regulatory ecosystem.

Key Complementarities

- NIS2 and CER provide dual pillars: cybersecurity and all-hazards resilience;
- CRA and CSA raise supply chain transparency and product security across digital components;
- Seveso III introduces safety management discipline for high-risk facilities integral to the energy lifecycle;
- Network codes ensure operational security and cross-border coordination, supporting resilience even during cyber disruptions.

Persistent Gaps

- Limited harmonisation between Seveso, CER, and NIS2 requirements at the facility level;
- Fragmented supervision, as cyber, physical, environmental, and Seveso authorities may operate in silos;
- Insufficient integration of hybrid threats, despite their growing relevance;
- Lack of OT and IioT specific cybersecurity certification scheme.

Emerging risk

- overlapping obligations due to poor integration of horizontal regulation and policies.

5. Assessing the Adequacy of the Current EU Framework for Energy Cyber Resilience

The European Union has significantly strengthened its regulatory architecture for cybersecurity and critical infrastructure resilience. However, as the energy sector undergoes rapid digitalisation, decentralisation, and integration with other critical systems, questions arise about whether existing instruments sufficiently address the multi-layered risks faced by modern energy infrastructures. This chapter evaluates the adequacy of the current framework across three dimensions: (1) coverage of the threat landscape, (2) coherence and alignment across regulatory instruments, and (3) suitability for addressing emerging systemic risks, including distributed architectures, hybrid threats, severe weather events, and safety-critical industrial processes.

5.1 Coverage of the Threat Landscape: Strengths and Gaps

The combined effect of NIS2, CER, the Cybersecurity Act, the Cyber Resilience Act, Seveso III, and the network codes provides broad coverage of cyber and non-cyber threats. Gaps remain in how these instruments address the realities of modern energy systems.

5.1.1 Distributed Architectures and Cybersecurity

NIS2 establishes horizontal cybersecurity obligations for essential and important entities, but the rapidly expanding ecosystem of distributed energy resources – solar photovoltaics, battery systems, smart inverters, electric vehicle chargers – sits only partially within its regulatory perimeter. Many DER devices are procured by prosumers or aggregators that may fall outside NIS2's classification, leaving significant portions of the low-voltage grid outside of the "compliance perimeter". Since Member States are currently transposing and implementing the NIS2, as the recital 20 of the NIS 2 stipulates, "*the Commission should, in cooperation with the Cooperation Group and after consulting the relevant stakeholders, provide guidelines on the implementation of the criteria applicable to microenterprises and small enterprises for the assessment of whether they fall within the scope of this Directive. The Commission should also ensure that appropriate guidance is given to microenterprises and small enterprises falling within the scope of this Directive. The Commission should, with the assistance of the Member States, make information available to microenterprises and small enterprises in that regard*".

The CRA increases baseline security requirements for digital products, but the Act alone cannot guarantee secure integration into energy systems.

As a result, the existing regulation does not fully cover the **cumulative systemic effects** arising from insecure or poorly coordinated DER deployments, despite growing concern about their use as potential vectors for coordinated cyber disruption.

5.1.2 Hybrid Threats, Physical Security, and Climate-Driven Risks

NIS2 primarily targets cyber risks, and although CER addresses physical, environmental, and hybrid threats, the practical integration of these domains remains challenging. Severe weather events, climate-induced stress on assets, and hybrid campaigns targeting energy operators are central vectors of disruption. CER explicitly recognises these hazards and threats, requiring resilience planning for extreme weather, natural disasters, sabotage, and hybrid activities.

Supervisory fragmentation between cyber authorities (implementing NIS2), civil protection and resilience authorities (implementing CER), and Seveso authorities (overseeing major accident hazards) risks producing **parallel risk assessments** that do not always converge. Energy operators may therefore struggle to produce a unified resilience strategy that incorporates cyber-physical interdependencies, grid stability concerns, climate-driven asset vulnerabilities, and hybrid threat scenarios.

5.1.3 Industrial Safety and Cyber-Physical Convergence

Seveso III ensures robust risk management for installations involving dangerous substances. However, Seveso's focus is traditionally on chemical and physical hazards, not on cyber triggers that could initiate major accident scenarios.

The growing integration of digital control systems into safety-critical environments – such as safety instrumented systems, remote valve controls, or tank monitoring – creates new vectors through which cyber operations can lead to Seveso-type physical consequences.

This represents a notable gap, as a cyber incident in a Seveso site could propagate through the broader energy system, affecting gas supply, LNG logistics, or cross-border transmission.

5.2 Coherence and Alignment Across Regulatory Instruments

While individual instruments have strong internal logic, the overall framework showcases areas of misalignment that affect energy cyber resilience.

By looking at the regulatory landscape analysed above, it can be stated that energy operators are subject to:

- NIS2 cybersecurity obligations;
- CER resilience obligations;
- Seveso III major accident prevention obligations (where applicable);
- CRA product lifecycle provisions;
- CSA certification and assurance provisions;
- Network Codes.

These instruments originate from different EU policy communities. Their coordination at the national level is not systematically ensured, given the fact that EU Member States also share a very uneven state of play and overall maturity in all those dimensions. Cybersecurity authorities, civil protection agencies, energy regulators, Seveso competent authorities, and market regulators each supervise different dimensions of resilience. Operators must therefore reconcile multiple supervisory expectations, which may create compliance inefficiencies and divergent interpretations of resilience.

The first and most persistent challenge is therefore governance fragmentation, which leads to the following consequences:

- Operators may receive conflicting or overlapping instructions, particularly regarding risk management, incident reporting, and supply chain oversight;
- Supervisory authorities often maintain separate threat models, leading to divergent assumptions about priorities, vulnerabilities, and acceptable mitigations;
- Cyber authorities focus on network and information systems; Seveso inspectors prioritise chemical hazards; CER authorities emphasise operational continuity and physical security; energy regulators focus on market stability.

Such fragmentation hinders a true understanding of systemic vulnerabilities and the reduction of the ability of Member States to anticipate, detect, and manage cross-sector disruptions.

The 2025 Digital Omnibus proposal, in case of approval, will have some systemic effects on the cyber resilience of the energy sector in two main domains: incident reporting harmonisation and alignment with the Cyber Resilience Act (CRA).

One of the most direct impacts on energy cyber resilience is the creation of a single EU incident reporting entry point, developed and operated by ENISA. This mechanism will consolidate reporting obligations currently scattered across:

- NIS2;
- CER Directive;
- GDPR;
- DORA;
- eIDAS,
- and the CRA vulnerability reporting framework.

Energy operators that qualify as essential or important entities under NIS2 and as critical entities under CER should no longer face parallel reporting streams to different authorities, thus reducing administrative friction, but more importantly, by improving cross-authority situational awareness, which is essential in complex, cascading cyber-physical incidents.

The envisaged mechanism should also strengthen the operational link between cyber incidents and physical disruption reporting, which is structurally weak as of today.

Finally, the Omnibus explicitly integrates the CRA vulnerability and severe incident reporting platform into the new single reporting entry point operated by ENISA, meaning that all digital components used in energy systems that fall within the scope of the CRA should structurally be connected to all the disclosure pipelines and coordinated response actions within the EU frameworks.

5.2.1 Lack of Energy-Specific Cybersecurity Standards

NIS2 and the CRA provide general principles and obligations for cybersecurity and product security, yet they do not define **energy-specific technical requirements for high-assurance digital components**. Operators are expected to implement "*appropriate and proportionate measures*", but without sector-specific guidance, this leads to heterogeneous interpretations.

Why the Lack of Technical Baselines Matters

- OT environments require security controls that differ from IT environments, including deterministic communication, real-time constraints, and safety interlocks;
- Lack of harmonisation weakens cross-border operational security, particularly for TSOs and DSOs engaged in coordinated system operations;
- Vendors can market products with minimal security guarantees, relying on proprietary designs and closed ecosystems.

Certification frameworks under the Cybersecurity Act offer a potential solution, but **no sector-specific scheme** yet exists for the energy domain. This contributes to systemic vulnerabilities in digital components that may have an impact on grid and supply chain stability.

5.2.2 Supply Chain Risk and Vendor Lock-In

NIS2 introduces mandatory supply chain risk management, the CRA reinforces lifecycle security, and the CSA provides mechanisms for certification. Despite these efforts, Europe's energy sector remains highly dependent on a small number of vendors whose proprietary ecosystems limit interoperability and constrain the ability of operators to diversify suppliers.

This ecosystem introduces two systemic challenges: **opacity** and **lock-in**.

Opacity

- Vendors may not disclose vulnerabilities, embedded components, or update pathways;
- Firmware, communication protocols, and diagnostic tools are often proprietary, limiting operator visibility;
- components may originate from jurisdictions with differing security standards.

Lock-In

- High switching costs prevent operators from replacing insecure technologies quickly;
- Long-term contracts, legacy interfaces, and integration dependencies reduce the feasibility of diversification;

- "As-a-Service" industrial platforms centralise critical functions under a single provider.

The current regulatory framework does not yet sufficiently incentivise interoperability, transparency, or the adoption of **trustworthy systems** – nor does it explicitly address the systemic risks created by concentrated vendor dependencies.

5.3 Suitability for Systemic Risks and Cross-Sector Dependencies

The final dimension of adequacy concerns the framework's capacity to address systemic risks, including cross-sector dependencies, distributed attack surfaces, and hybrid threats.

5.3.1 Cross-Sector and Cross-Border Interdependencies

The energy sector depends on telecommunications networks, satellite-based timing systems, cloud services, ports, LNG logistics, chemical safety systems, and cross-border transmission corridors. Although the CER Directive requires Member States to consider cross-border dependencies, and Network Codes enhance operational coordination, systemic dependencies involving digital services, space-based infrastructure and global supply chains are not yet fully integrated into regulatory supervision. In the context of supply chain continuity and third-party risk management, a DORA-like[34] regulatory approach – modelled on the framework adopted for the financial sector – could be explored for the energy domain. Such an approach would introduce sector-specific requirements on digital vendors and critical service providers, including enhanced due diligence obligations, contractual rights of audit, mandatory exit and substitution strategies, the identification of systemic providers, and structured arrangements for mutual operational support. This approach could strengthen the digital operational resilience of the energy sector across its increasingly complex and interconnected value chain.

As anticipated earlier, space-based services also remain insufficiently integrated into resilience planning. Satellite timing, Earth observation, and satellite communications are already critical enablers of modern grid operations, yet current regulatory frameworks on the resilience of critical entities still focus predominantly on ground-based segments, leaving orbital assets comparatively under-addressed. With the deployment of new space programmes such as IRIS²[35], and the progressive enhancement of existing ones such as the Galileo Early Warning Satellite Services (EWSS)[36], operators of essential services should be provided with a deeper and more structured awareness of space-related risk scenarios. This is necessary to trigger the development of resilient strategies, contingency

[34] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

[35] IRIS² (Infrastructure for Resilience, Interconnectivity and Security by Satellite) is the EU's new secure satellite connectivity programme aimed at providing resilient, encrypted broadband services for governmental users and critical infrastructure operators while strengthening Europe's strategic autonomy in space-based communications.

[36] The Galileo Early Warning Satellite Service (EWSS) is a safety-oriented augmentation of the EU's Galileo Global Navigation Satellite System, designed to support early warning functionalities for time-critical civil protection and infrastructure monitoring applications, thereby enhancing resilience against cascading and rapidly evolving threats.

planning, and tactical response measures in the event that space-enabled services are degraded, disrupted, or deliberately targeted.

5.3.2 Integration of Cyber, Physical, and Climate Resilience

CER's all-hazards approach represents significant progress, but the **practical integration** of cyber, physical, and climate considerations requires operational clarity. Climate adaptation strategies rarely include cyber considerations; cybersecurity strategies rarely consider climate extremes; Seveso assessments rarely incorporate cyber triggers; and emergency planning frameworks do not always address hybrid threat scenarios that combine physical sabotage, cyber intrusion, and disinformation.

This fragmentation limits the ability of current regulation to address **compound, cascading shocks**.

5.3.3 Digitalisation Pace and Supervisory Capacity

The digital transformation of the energy system is accelerating faster than regulatory implementation or supervisory capacity. As operators adopt AI-enabled forecasting tools, automation platforms, and cloud-based industrial services, regulators face increasing challenges in ensuring consistent oversight across diverse digital environments.

Supervisory authorities often lack structured mechanisms to verify:

- the resilience of distributed intelligent devices;
- the security posture of vendors and third-party developers;
- the quality of software update and vulnerability disclosure processes.

These gaps highlight the need for regulatory tools capable of providing verifiable assurance, including the possible future role of sector-specific cybersecurity certification schemes for digital energy components.

6. Towards a Coherent EU Approach to Embedding Cyber Resilience in Energy Regulation

The analyses presented throughout this paper demonstrate that strengthening cyber resilience in the European energy sector requires a multi-level strategy that aligns regulatory evolution, assurance mechanisms, and operational harmonisation. This concluding chapter synthesises the core findings into three final areas of action: the regulatory dimension, the certification dimension, and the tactical and harmonisation dimension. Together, these areas provide a roadmap for embedding cyber resilience more deeply into Europe's energy governance framework.

6.1 The Regulatory Dimension

The regulatory architecture governing cyber resilience in the European energy sector has entered a decisive phase. With the NIS2 and CER Directives recently adopted and now moving through national transposition and implementation, and with the Cyber Resilience Act (CRA) expected to become fully enforceable in 2027, the current policy lifecycle is still in its early operational maturity stage. Against this background, regulatory evolution should follow a sequenced and realistic logic, structured around two short-term consolidation actions and one long-term structural action.

Short-Term Action 1 – Consolidate Implementation and Enable Maturity to Emerge

Given the novelty and breadth of the current framework, the immediate priority should be to allow results to emerge and regulatory maturity to consolidate, rather than to pursue premature legislative layering. Member States currently display very uneven levels of preparedness, institutional capacity, and supervisory integration in implementing NIS2 and CER. In this phase, the imperative should be to:

- Support stakeholders – operators, regulators, and competent authorities – in fully executing their new obligations;
- Strengthen harmonisation levels across the Union through coordinated guidance, peer exchange, and structured support;
- Reduce interpretative fragmentation in areas such as supply chain security, incident reporting, cross-border dependencies, and hybrid threat treatment.

This phase should be characterised by regulatory stability combined with intense operational support, including guidance, capacity building, and supervisory coordination. Only once consistent minimum maturity levels are achieved, further regulatory escalation will be both effective and proportionate.

Short-Term Action 2 – Establish a European Programme for Critical Entities Resilience (EPCER)

The consolidation of the current regulatory cycle would be significantly reinforced by relaunching a structured European Programme for Critical Infrastructure Protection (EPCIP), updated to reflect today's cyber-physical, hybrid and resilience-driven environment.

Between 2008 and 2020, EPCIP provided a unique trusted platform where EU institutions, national authorities, operators, standardisation bodies, and academia could collectively develop methodologies, exchange best practices, conduct exercises, and harmonise security approaches. That programme played a decisive role in preparing the ground for today's NIS and CER framework and community.

The EPCIP included the so-called "external dimension" which was a very forward-looking action aimed at including "neighbouring countries of the EU" (with priority on the Second Enlargement Agenda) in some of the activities of the programme. This specific action led to several workshops which allowed exchanges on trans-boundary challenges faced by neighbouring countries and in an important platform for the exchange of best practices to be perused by countries that are heavily interconnected with the EU and on which the EU relies too.

A new European Programme for Critical Entities Resilience (EPCER) would directly support Short-Term Action 1 by:

- Maintaining and further expanding the EU community engaged in critical entity resilience and cybersecurity;
- Facilitating further structured information sharing across sectors and Member States;
- Enabling joint stress tests and table-top exercises on cyber-physical and hybrid scenarios;
- Supporting the operational dissemination of applied research from EU-funded projects;
- Allowing cross-border pilot projects on resilience technologies and governance models;
- Providing a coordination space for horizontal and vertical regulatory issues.

Such a programme would serve as both a strategic stabiliser and an operational accelerator of the current regulatory lifecycle, ensuring that NIS2 and CER evolve from compliance instruments into effective enablers of resilience in practice. For this reason, it should not be deferred to the 2028–2034 Multiannual Financial Framework (MFF), but rather be launched as early as possible.

Long-Term Action 3 –DORA-Like Framework for Lifeline Infrastructures

Once a higher level of regulatory and operational maturity has been achieved across the Union, the next policy cycle should move decisively toward structural integration.

At that stage, the introduction of NIS3 and CER2 as reinforced horizontal instruments, and a DORA-like regime tailored to lifeline critical infrastructures, starting with the energy sector, could represent the logical evolution of EU resilience governance.

A DORA-style framework for energy would go beyond traditional cybersecurity compliance and introduce:

- Mandatory vendor due diligence;
- Contractual rights of audit on critical ICT and OT suppliers;
- Enforceable exit and substitution strategies;
- Identification and supervision of systemic digital service providers in the EU;

- Structured mutual support and operational continuity mechanisms.

Positioning such a framework only after the consolidation of NIS2, CER and CRA would ensure regulatory proportionality, avoid overburdening operators during the current transition, and anchor the next generation of resilience regulation on verified implementation experience.

6.1.1 Regulatory Trajectory in Synthesis

Taken together, these three actions define a progressive regulatory trajectory:

1. Stabilise and mature what already exists (NIS2, CER, CRA implementation);
2. Rebuild a European operational coordination backbone (EPCER);
3. Only then, structurally upgrade the model through NIS3, CER2, and a DORA-like regime for lifeline infrastructures.

This sequence protects the Union from regulatory saturation while ensuring that the energy sector's cyber resilience evolves in step with the growing complexity of its digital, physical, and geopolitical exposure.

6.2 Certification Dimension

Security assurance, trustworthiness, and vendor accountability are essential pillars of cyber resilience. The current mix of horizontal and sectoral requirements lacks the sector-specific focus needed for high-assurance digital components in the energy domain.

Action 4: Task ENISA With Developing a Dedicated Cybersecurity Certification Scheme for Energy Sector Devices

The European Commission should mandate ENISA, under the Cybersecurity Act, to develop a sector-specific cybersecurity certification scheme for digital components used in energy systems. Such a scheme would significantly improve trustworthiness and reduce vendor lock-in by:

- Ensuring that international manufacturers test devices against EU requirements before market entry;
- Reducing the likelihood that devices contain insecure firmware, flawed hardware components, or software vulnerabilities;
- Enabling regulators and operators to rely on verified, transparent assurance levels;
- Enabling operators to improve the requirements for procurement of digital components;
- Supporting market diversification by making security assurance a differentiator;
- Aligning certification with the lifecycle obligations introduced by the Cyber Resilience Act.

Certification would shift the burden of proof towards suppliers, strengthen the EU's resilience posture, and create a clearer path for secure-by-design products within the energy sector.

This action is already foreseen in the current Union Rolling Work Programme for Cybersecurity Certification and, considering the urgency of supporting the ongoing NIS2, CER and CRA implementation cycle, it should be initiated without delay. Building on the experience gained with the implemented EUCC scheme and the candidate EUCS scheme, **the Commission should also pilot an accelerated certification development track, with the objective of significantly reducing the time-to-market of candidate schemes by limiting the preparatory phase to a maximum duration of one year**.

6.3 Tactical and Harmonisation Dimension

Operational clarity is essential for ensuring that risk assessments, supervisory tasks, and resilience planning converge toward coherent outcomes across the Union. Despite recent progress, further guidance is required to ensure consistent interpretation and implementation.

Action 5: Produce Enhanced EU Guidance on the Interaction Between Risks, Hazards, and Threats

Foreign international experiences, like the one of the United States of America with the National Institute for Standards and Technology, have shown the capability to enforce security and resilience measures through technical standards, in many cases also by avoiding the need to promulgate dedicated regulations. By following this approach, the European Commission, ENISA, and relevant agencies should foster the production of **cross-cutting, practical guidance and technical standards** addressing how operators should integrate cyber risks, physical hazards, climate-driven events, and hybrid threats into a unified analytical framework. This guidance should clarify:

- Methodological intersections between NIS2 cybersecurity assessments and CER all-hazards analyses;
- The integration of Seveso major-accident triggers with cyber-physical scenarios;
- The treatment of interdependencies such as satellite-based timing, supply chains, and cross-border energy flows;
- Expectations for addressing hybrid threat activity, including disinformation, coercive economic measures and targeted sabotage.

Such guidance would reduce fragmentation, enhance harmonisation across Member States, enhance measurability of progress achieved and support operators in building comprehensive, risk-informed resilience strategies.

6.4 Final Reflections

The European Union stands at a decisive moment in shaping the future of cyber resilience in its energy system. By strengthening regulatory coherence, creating trusted certification pathways and providing harmonised operational guidance, the Union can advance towards a resilience model that is systemic, proportionate and future-proof. These actions, taken together, could help ensure that Europe's energy system remains secure, reliable, and resilient in the face of an increasingly complex and contested threat and hazard landscape.

7. References

COMMISSION DELEGATED REGULATION (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows

COMMISSION REGULATION (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration, Official Journal of the European Union 28.11.2017

European Commission (2024), Union Rolling Work Programme for European Cybersecurity Certification, SWD(2024) 38 final, Brussels.

European Commission (2025), Proposal for a Council Recommendation on an EU Blueprint on Cybersecurity Crisis Management, COM(2025) 66 final, Brussels.

European Commission (2025), Proposal for a Regulation amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) , COM(2025) 837 final, Brussels.

European Commission – Joint Research Centre (2016), Space Weather and Critical Infrastructures: Findings and Outlook, EUR 28237 EN, Publications Office of the European Union, Luxembourg, doi:10.2788/152877.

European Commission, Joint Research Centre, Lentini, A., Eklund, G., Corbane, C., Asikainen, T., Ronco, M., Urso G., Poljansek, K., Soler Garrido, J., Griesinger, C.B., Reina, V., Spigolon, R., Steri, G., Linge, J., Kotseva, B., Masante, D., Santini, M., Proietti, C., Barantiev, D., Salvitti, V., Destro, E., Mastronunzio, M., Hrast Essenfelder, A., Toreti, A., Salamon, P., D'Angelo, C., Vousdoukas, M., Crippa, M., Pisoni, E., Belis, C., Carravieri, A., Ruiz-Orejón, L.F., Mendes, C., Robuchon, M., Sanchez Arjona, I., Tsionis, G., Schuh, L., Spagnolo, L., Orfei L., Petrillo M., Kephalopoulos, S., Coecke, S., Aschberger, K., Schirinzi, G., Maddalon, A., Valsesia, A., Armas, F., Guglielmelli, A., De La Rosa Blul, J.C., Magrotti, G., Cardarilli, M., Petit, F., Theron, J., De Angelis, A., Krausmann, E., Wood, M., Van Wijk, L., Koutelos, K., Schvitz, G., Galariotis, I., Gentile, C., De Girolamo, L., Duta, A., Caravaggi, I., Thau, A., Bagi, J., Larcher, M., Karlos, V., Ruiz Moreno, A., Baruth, B., Rembold, F., Sedano, F., Scionti, N., San-Miguel, J., Durrant, T., Boca, R., Maianti, P., Oom, D., Branco, A., De Rigo, D., Suarez Moreno, M., Ferrari, D., Roglia, E., Broglia, M., Belmonte, M., Pingsdorf, J., Kajander, N., Majorano Sarapo, F., Greidanus, H., Montanari, E., Piccinini, P., Roman-Cuesta, R.M., Dentener, F., Galmarini, S., De Groeve, T., Maenhout, G., Analysis of Risks Europe is facing, Publications Office of the European Union, Luxembourg, 2025, https://data.europa.eu/doi/10.2760/0176850, JRC141673

European Parliament and Council of the European Union (2012), Directive 2012/18/EU on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC, Official Journal of the European Union, L 197, 24.7.2012.

European Parliament and Council of the European Union (2019), Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), Official Journal of the European Union, L 151, 7.6.2019.

European Parliament and Council of the European Union (2022), Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Official Journal of the European Union, L 333, 27.12.2022.

European Parliament and Council of the European Union (2022), Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Official Journal of the European Union, L 333, 27.12.2022.

European Parliament and Council of the European Union (2024), Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), Official Journal of the European Union, L, 20.11.2024.

European Union Agency for Cybersecurity (ENISA) (2025), ENISA Threat Landscape 2025, Publications Office of the European Union, Luxembourg, October 2025, ISBN 978-92-9204-723-8, DOI: 10.2824/1946374.

Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/37899, JRC129019.

Paul Theron, Introduction to the European IACS components Cybersecurity Certification Framework (ICCF), Publications Office of the European Union, doi:10.2760/717579

Theron, P. and Lazari, A., The IACS Cybersecurity Certification Framework (ICCF). Lessons from the 2017 study of the state of the art., EUR 29237 EN, Publications Office of the European Union, Luxembourg, 2018, ISBN 978-92-79-85968-7, doi:10.2760/856808, JRC111611

THERON, Paul; RUIZ GUALDA, Jose Francisco; BOSWELL, Tony; BRUN, Jean-Michel; CASCELLA, Roberto; F., Luis; FREEMAN, Matthew; GONZALEZDE, Sergio; GORSKI, Janusz; INZERILLI, Tiziano; JANSEN, Martijn Michiel; JARDIM, Mario Roberto; KOBES, Pierre; KREUTZMANN, Helge; MENTING, Jos; PUCCETTI, Armand; QUEMARD, Jean-Pierre; QUERREC, Emmanuel; SADMI, Franck; THEUERZEIT, Michael; VENTER, Razvan; WOLLENWEBER, Kai; WYBOU, Nathanael, Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS), European Commission, Ispra, 2020, JRC121520

8. List of Acronyms

AI – Artificial Intelligence

CER – Critical Entities Resilience

CERRE – Centre on Regulation in Europe

CIA / C-I-A – Confidentiality, Integrity, Availability

CRA – Cyber Resilience Act

CSA – Cybersecurity Act

DSO – Distribution System Operator

DORA – Digital Operational Resilience Act

DER – Distributed Energy Resource

EPCER – European Programme for Critical Entities Resilience

EPCIP – European Programme for Critical Infrastructure Protection

ERNCIP – European Reference Network for Critical Infrastructure Protection

EU – European Union

EUCC – European Union Cybersecurity Certification

EUCS – European Union Cybersecurity Scheme for Cloud Services

EWSS – Galileo Early Warning Satellite Services

GNSS – Global Navigation Satellite System

ICT – Information and Communication Technologies

IIoT – Industrial Internet of Things

IPCR – Integrated Political Crisis Response

IACS – Industrial Automation and Control Systems

IRIS² – Infrastructure for Resilience, Interconnectivity and Security by Satellite

IT – Information Technology

JRC – Joint Research Centre

LNG – Liquefied Natural Gas

MFF – Multiannual Financial Framework

NERC CIP – North American Electric Reliability Corporation – Critical Infrastructure Protection

NEMO – Nominated Electricity Market Operator

NIS2 – Network and Information Security Directive (recast)

OT – Operational Technology

PLC – Programmable Logic Controller

SBOM – Software Bill of Materials

SCADA – Supervisory Control and Data Acquisition

Seveso III – Directive 2012/18/EU on the control of major-accident hazards

TSO – Transmission System Operator

About CERRE

Providing high quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) is a not-for-profit think tank. It promotes robust and consistent regulation in Europe's network, digital industry, and service sectors. CERRE's members are regulatory authorities and companies operating in these sectors, as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach covering a variety of markets, e.g., energy, mobility, sustainability, tech, media, telecom, etc.;
- the widely acknowledged academic credentials and policy experience of its research team and associated staff members;
- its scientific independence and impartiality; and,
- the direct relevance and timeliness of its contributions to the policy and regulatory development process impacting network industry players and the markets for their goods and services.

CERRE's activities include contributions to the development of norms, standards, and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological, and social environment. CERRE's work also aims to clarify the respective roles of market operators, governments, and regulatory authorities, as well as contribute to the enhancement of those organisations' expertise in addressing regulatory issues of relevance to their activities.

About the Author

Alessandro Lazari is a Postdoctoral Researcher and Fellow at the Centre for Interdisciplinary Research on Critical Infrastructure Security and Resilience (CRISR), University of Salento, specialised in Critical Infrastructure Protection, Resilience, and Cybersecurity. He is Advisor to the Office of the Military Advisor at the Presidency of the Council of Ministers, the national authority for Critical Entity Resilience in Italy. He holds a Master's Degree in Law from the University of Bologna, a specialisation in Law from the University of Lecce, and a PhD in Computer Engineering, Multimedia and Telecommunications from the University of Florence.

cerre Centre on Regulation in Europe

Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu

Centre on Regulation in Europe (CERRE)
CERRE Think Tank
CERRE Think Tank