DIGITAL INTERDEPENDENCE AND STRATEGIC RISK: HYBRID THREATS IN EUROPE'S ENERGY SECTOR

DOI: https://doi.org/10.37458/nstf.27.2.4
Original scientific paper
Received: September 9, 2026
Accepted: November 5, 2026

Genny Dimitrakopoulou, LLM, MSC, MA*

Abstract: Europe's highly digitalised, interdependent energy systems face rising exposure to hybrid attacks. As OT/IT convergence increases cyber-physical incidents propagate across borders, triggering not only operational but also geopolitical disruption. This paper analyses how perpetrators exploit the seams between the digital interconnections and legacy infrastructure. It evaluates recent case studies and presents

* Genny Dimitrakopoulou is a Senior Cyber Security Researcher and Coordinator of Outreach and Communication at the Center for Security Studies (KEMEA). She is the author of a security e-book, as well as the Greek delegate for the International MediaPoli Organisation for police mediation. She is a guest Lecturer at the Panteion University in EU Law, and a member of the Scientific Committee of the international CBRNe R&I conference in the domain of crisis and risk management. Email address: g.dimitrakopoulou@kemea-research.gr

pertinent EU resilience frameworks, proposing the use of autonomous aerial systems as a useful tool for safeguarding physical nodes. It concludes by arguing for a multi-domain approach to protect European energy resilience.

Keywords: Critical Infrastructure Protection (CIP), Hybrid Threats, Cyber-Physical Security, Energy Resilience, Digital Interdependence, UAVs

Introduction

Over the past decade, Europe's energy systems have been quietly but steadily transformed into strategic terrain. What used to be treated as a largely technical domain has become fertile soil for geopolitical competition to unfold in subtle, and often ambiguous, ways. The green transition, which was expected to modernise and decarbonise Europe's energy front, has accelerated digitalisation to a degree that was not fully anticipated. Thus, as digital interdependencies deepen, so does systemic fragility[1]. This fragility is not simply a byproduct of technological change. It is shaped by broader geopolitical dynamics, such as fragmented global energy markets, competition over critical raw materials, and persistent hybrid activity targeting European critical infrastructure. For instance, Russia's long term posture toward European energy networks has demonstrated that energy can be used as a tool of

[1] Goldthau, A., Keim, M., & Westphal, K. (2018). The geopolitics of energy transformation: governing the shift: transformation dividends, systemic risks and new uncertainties. (SWP Comment, 42/2018). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. https://nbn-resolving.org/ urn:nbn:de:0168-ssoar-60135-0

pressure and signalling[2]. At the same time, non-state actors have become increasingly more capable of exploiting digital vulnerabilities and gaps between the seams, often with limited resources but significant strategic leverage. In this environment, disruptions in energy systems carry consequences that extend far beyond the localised operational inconvenience and functional downtime; these disruptions actively manipulate public anxiety, influence political decisions and, ultimately, reshape the strategic decisions of adversarial states. In game theory terms, hybrid incidents alter the payoff results: they increase the political cost of inaction, reduce the perceived stability of the status quo, and push states to reconsider their optimal strategies under heightened uncertainty.

In spite of these compounding risks, contemporary analysis frequently treats technical vulnerabilities and macroeconomic statecraft as two isolated phenomena, which leaves a critical gap at the intersection of operational engineering and geopolitical strategy. The objective of this paper is to address and bridge this gap, between the operational and technical vulnerability evaluations, and the strategic security assessment. Its scientific contribution lies in the provision of a multi-layered analytical framework that endeavours to link macro-level EU regulatory evolution with micro-level operational technologies, specifically inspecting where and how autonomous systems can realistically mitigate vulnerabilities within the broader, defense structure. Using this framework, the study explores the following

[2] For a comprehensive account, see Galeotti, M. (2023). The weaponisation of everything: A field guide to the new way of war. Yale University Press. https://yalebooks.yale.edu/book/9780300270419/the-weaponisation-of-everything/

central research question: How does the digital and cross-border interdependence of Europe's energy systems change the structure of hybrid security risks, and under what conditions can autonomous surveillance systems contribute to the resilience of critical infrastructure?

Finally, to ground this theoretical framework, it evaluates a practical countermeasure: deploying state-of-the-art aerial systems to safeguard energy systems' protection and resilience. The aim is to offer a perspective that is both theoretically grounded and operationally relevant, reflecting the needs of a continent that is currently navigating a complex and contested energy future.

Methodology

This study adopts a qualitative, conceptual analysis paired with case studies' analysis to identify the intersection of technological interdependence with hybrid warfare within the energy critical infrastructure. The research methodology is structured into three integrated phases: first, a brief introduction into hybrid threat theory, followed by the Information Technology[3] (IT) / Operational Technology[4] (OT) convergence, and the evolving EU regulatory frameworks; second, a qualitative case analysis of emblematic cyber-physical incidents representative of hybrid attacks; and third, an

[3] Information Technology comprises of all the systems that run the digital environment of energy infrastructure, e.g., the corporate computers, email servers, logistics systems, databases, websites, cloud services, etc.

[4] Operational Technology is the totality of the systems that physically operate energy infrastructure e.g., the substations, pipelines, turbines, centrifuges, SCADA systems, and PLCs (programmable logic controllers).

assessment that links new-generation technical vectors to strategic outcomes.

To ensure accuracy and analytical validity, five historical cyber-physical incidents have been selected, based on four criteria: (a) the systemic relevance and direct impact on the energy infrastructure, (b) the operational convergence of IT and OT domains, (c) the presence of cascading effects, and (d) the reveal of a clear geopolitical, strategic intent by the perpetrators. Under these criteria, the cyber-attacks on the Ukrainian power grid (2015-2022), the NotPetya malware outbreak (2017), the Colonial Pipeline ransomware attack (2021), the Shamoon virus deployment (2012), and the Stuxnet destruction of nuclear centrifuges (2010) were selected as characteristic cases that represent different typologies of critical infrastructure disruption.

The analysis traces the linear relationship between a technical/technological attack (e.g., malware infiltration, protocol exploitation) to tangible operational consequences (e.g., grid malfunction, IT paralysis) and, ultimately, to strategic impact (e.g., political coercion, economic/political instability, societal panic) and the need for prompt detection and containment of the incidents. It demonstrates how digital interdependence reshapes strategic risk in Europe's energy sector by mapping out the current hybrid threat landscape before tackling the operational friction caused by the convergence of Operational Technology (OT) and Information Technology (IT). Finally, to determine whether autonomous aerial systems can actually lower these security risks, the paper evaluates if and how drone capabilities (such as rapid scanning and equipment

checks) can strengthen the specific resilience indicators identified in the five case studies.

Hybrid Threats as Strategic Action

Europe's energy ecosystem is no longer a neutral technical space, but a strategic asset whose vulnerabilities can be leveraged in hybrid conflict environments that produce the above-mentioned effects. A cyber-physical incident affecting a transmission substation or a pipeline can trigger price volatility, destabilise society, create panic buying, and cause diplomatic tension. In this context, hybrid warfare is defined not by a single, straightforward military action, but as the blend of conventional and unconventional, digital/cyber, and economic instruments deployed by adversaries to exploit systemic vulnerabilities while remaining below the threshold of traditional warfare[5]. This complexity stems from the fact that hybrid threats occupy a space that is deliberately ambiguous. They are neither conventional military operations nor purely civilian disruptions. While operating in secrecy and under the threshold of war, they combine an array of destructive elements: cyber intrusions, disinformation campaigns through social media, economic pressure, and covert physical sabotage in ways designed to stay undetected and unattributable to specific persons, groups, or countries. This opacity is analogous to their effectiveness. It complicates attribution, delays

[5] Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies, and Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats, & European Commission's Joint Research Centre (JRC). (2021). The landscape of hybrid threats: A conceptual model. Publications Office of the European Union.

response, and creates uncertainty among policymakers and operators[6].

NATO's definition of hybrid threats emphasises the integration of military, paramilitary, and civilian measures[7]. The European Union's Hybrid Toolbox frames hybrid campaigns as multidomain operations aimed at exploiting systemic vulnerabilities[8]. Both perspectives recognise that hybrid threats are not isolated incidents but sustained strategic actions. They are designed to erode political resilience, undermine social trust, and shape the behaviour of states and societies. To that end, energy systems are particularly attractive targets for hybrid actors. They "sit" at the intersection of national security, economic stability, and everyday societal functioning. A disruption in an electricity grid or a gas pipeline can produce cascading effects across multiple sectors and states. Effects are amplified by the interconnected nature of Europe's energy networks, where a disturbance in one subsystem can propagate across borders and destabilise regional markets. Hybrid attackers target these interdependencies and use timing to infiltrate the seams between technical domains. A well-timed cyber intrusion into a renewable energy forecasting system, for example, can create imbalances in regional grids. A supply chain compromise affecting a widely used software vendor can have a rippling effect across numerous operators. And this is exactly how hybrid incidents succeed in penetrating infrastructure: they manipulate the structure

[6] NATO. (2026, January 29). Countering hybrid threats. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

[7] Ibid.

[8] Council of the European Union. (2026). Hybrid threats. https://www.consilium.europa.eu/en/policies/hybrid-threats/

of modern energy systems - systems that are efficient, interconnected, and therefore vulnerable and attractive to perpetrators.

Digital Interdependence and Systemic Fragility

Digital interdependence has now become one of the most shaping characteristics of European (and global) energy systems. Green transition has further accelerated the integration of digital technologies into energy operations in the form of sensors, automation platforms, cloud-based tools for forecasting, and importantly remote access systems. While all of these technologies increase efficiency and enable cross-border coordination, they also create tightly coupled systems where disruptions can spread rapidly[9]. A compromise at even the first, node level, an IT intrusion, a supplier breach, or a ransomware attack where a system is infected with malware, could all escalate into subsystem interruption. Local operations can be (and have been) destabilised by manipulation of SCADA[10] systems, interference with renewable energy forecasting[11], or tampering with protection relays can destabilise local operations.

Once a subsystem is compromised, cross border propagation, and hence escalation, becomes likely particularly through interconnectors, shared vendors,

[9] International Energy Agency. (2025). Energy and AI: World Energy Outlook special report. https://iea.blob.core.windows.net/assets/de9dea13-b07d-42c5-a398-d1b3ae17d866/EnergyandAI.pdf

[10] SCADA stands for Supervisory Control And Data Acquisition. It describes all the systems that monitor, control, and automate industrial processes, in the energy and other sectors.

[11] Renewable energy forecasting predicts how much electricity the renewable sources (wind and solar) will generate in the future. Forecasting is important because these sources depend on weather, which is a parameter that cannot be controlled.

and pertinent regional balancing mechanisms. The final stage of this systemic fragility is societal impact. When a technical incident happens, it sets off a chain reaction, where market prices spike, public anxiety increases, and state or non-state perpetrators can easily exert strategic leverage over pressured policymakers. We have seen that energy disruptions can influence electoral dynamics[12], shape public trust in institutions[13], and alter the strategic position of states. Hybrid actors exploit this dynamic to the fullest, as well as the indisputable fact that modern societies depend on uninterrupted energy flows, not only for vital and everyday economic activities, but also for psychological security[14].

The systemic fragility of Europe's energy systems is therefore not merely a technical challenge, any longer. It is a strategic vulnerability that needs to be proactively mitigated. To address it, we need to reconceptualise energy security by integrating digital resilience, cross-border coordination, joint preparedness exercises, and autonomous operational capability. Ultimately, European strategic stability is as strong as its weakest digital node. If the continent cannot withstand these grey zone disruptions, its broader energy security remains unattainable.

[12] Freitag, Nils, The Political Consequences of Energy Price Shocks: Evidence from Berlin, July 01, 2026. Available at SSRN: https://ssrn.com/abstract=7165539 or http://dx.doi.org/10.2139/ssrn.7165539 and Brännlund, A., & Peterson, L. (2024). Power politics: How electric grievances shape election outcomes. Ecological Economics, 217, 108077. https://doi.org/10.1016/j.ecolecon.2023.108077

[13] Wang, Q., Ren, F., & Li, R. (2024). Geopolitics and energy security: A comprehensive exploration of evolution, collaborations, and future directions. *Humanities and Social Sciences Communications*, *11*(1), 1071. https://doi.org/10.1057/s41599-024-03507-2

[14] Rubin, G. J., & Rogers, M. B. (2019). Behavioural and psychological responses of the public during a major power outage: A literature review. *International Journal of Disaster Risk Reduction*, *38*, 101226. https://doi.org/10.1016/j.ijdrr.2019.101226

The Hybrid Threat Landscape

The hybrid threat landscape affecting Europe's energy systems has become more complex and more aggressive. The European Union Agency for Cybersecurity's (ENISA) recent data confirm that ransomware incidents increased sharply between 2025 and 2026, reaching more than two thousand cases across thirty-one countries.[7] Manufacturing, energy, and utilities will continue to remain among the most targeted sectors and weakest links in the societal chain. Further, monthly attack rates have risen, and supply chain compromise continues to be a dominant route. The Miljödata incident[15], which affected hundreds of municipalities and universities, demonstrated how a single compromised vendor can destabilise multiple public sector entities[16].

Energy operators rely on complex supply chains involving, for example, software vendors, cloud providers, sensor manufacturers, and maintenance contractors. Each link in this chain represents a potential entry point for hybrid, cyber criminals. The financial impact of such incidents is significant, as recovery costs for major outages now exceed three million euros, once operational and reputational losses are included[17]. Critical infrastructure incidents reported under the NIS[18]

[15] Data Breach Registries & Monitoring Services, Have I Been Pwned. (2025, September). Data breach registry: Miljödata https://haveibeenpwned.com/Breach/Miljodata

[16] DIESEC. (2025, October 29). *Ransomware in the supply chain: Swedish IT supplier gets hit*. https://diesec.com/2025/10/ransomware-in-the-supply-chain-swedish-it-supplier-gets-hit/

[17] Agency for the Cooperation of Energy Regulators. (2026). Cybersecurity network code for electricity. https://www.acer.europa.eu/electricity/cybersecurity

[18] European Commission, Directorate-General for Communications Networks, Content and Technology. (2026). NIS2 Directive: Securing network and information systems. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Directive have also increased, with a substantial proportion classified as intentional. ENISA warns that successful cyberattacks can cascade into health and emergency service outages, underscoring the systemic nature of contemporary hybrid threats[19].

Hybrid campaigns progressively blend digital intrusion, physical sabotage, and information manipulation[20]. Disinformation about energy prices, outages, or supply shortages can amplify the impact of technical incidents, creating public unrest, panic buying, and therefore political pressure. In this way, hybrid actors manage to exploit uncertainty, ambiguity, and the difficulty of attribution to achieve their objectives without triggering conventional responses. Understanding this landscape is crucial, and requires a multidimensional approach that integrates technical and legal knowledge, strategic analysis, and policy evaluation. It also forces the recognition that hybrid threats evolve in response to technological change, regulatory adaptation, and geopolitical dynamics[21], consequently multi-disciplinary response teams must become the norm.

Operational Technology / Information Technology Convergence: An Expanded Attack Surface

A central development in Europe's energy scene has been the gradual dissolution of the traditional boundary between Operational Technology (OT) meaning the physical energy infrastructure, and Information

[19] European Union Agency for Cybersecurity. (2025, October 1). ENISA Threat Landscape 2025. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[20] Digital Intrusion and Critical Infrastructure Cyber-Attacks, Brantly, A. F. (2021). The cyber-physical nexus: Assessing risks to critical infrastructure. Journal of Cyber Policy, *6*(2), 184–202. https://doi.org/10.1080/23738871.2021.1983572

Technology (IT) i.e., all the digital systems. Historically, OT environments were built like digital fortresses. The essence of security was total physical isolation with an absolute focus on maintaining predictable control over infrastructure like pipelines and substations. Since connectivity was limited, external access was tightly controlled[22]. This architecture has changed dramatically[23]. As energy operators are modernising their systems to make them more efficient, OT environments are increasingly connected to corporate networks, cloud-based services, and remote access platforms.

Smart grid technologies[24] (which rely on real time data flows and automated decision making) have further accelerated this convergence. Sensors, remote terminal units, and Programmable Logic Controllers (PLCs[25]) now interact with digital platforms that were never originally intended to interface with physical infrastructure - a fact that creates an added layer of complications on its own. This shift has expanded the attack surface in ways that are not always visible at first glance. Legacy SCADA systems, many of which were designed decades ago, are now for the first time exposed to modern attacks, perpetrated by actors who possess both the technical expertise and the strategic reasons to

[22] Cybersecurity and Infrastructure Security Agency. (2026). Energy sector: Critical infrastructure security and resilience. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector

[23] Sectech Solutions. (2024, September 3). *The intersection of OT and IT security in the energy sector*. https://www.sectechsolutions.co.uk/post/the-intersection-of-ot-and-it-security-in-the-energy-sector

[24] Strojny, J., & Kacorzyk, P. (2025). Economic Aspects of Energy Production, Distribution and Consumption. *Energies*, *18*(6), 1369. https://doi.org/10.3390/en18061369

[25] A PLC is a field-level controller that executes real-time operations in energy infrastructure, such as regulating voltage, reading sensor data, etc.

exploit them. Internet of Things (IoT)[26] enabled devices, often deployed to improve efficacy or to reduce operational costs, may also become low cost entry points for cyber intruders. Cloud-based services offer both scalability and convenience, but they also introduce remote access vectors that hybrid attackers may manipulate[27].

Surveys consistently show that most energy companies realise their increased OT vulnerability, and recognise that OT security lags behind IT[28]. This lag reflects the deeper structural differences in how OT and IT systems are designed, maintained, and operated. OT is anchored in physical safety, whereas IT prioritises network flexibility. Therefore, when these two domains converge, the resulting environment is often more complex than either domain alone. This complexity is what the perpetrators target, as they know that an intrusion into an IT system is the as a stepping stone toward OT manipulation. The Colonial Pipeline incident demonstrated this dynamic clearly: although the ransomware attack targeted corporate IT systems, the pipeline operator shut down the system as a precaution, which in turn caused fuel shortages, and economic and societal disruption[29]. This serves as lesson learned: in a converged environment, IT intrusion can cascade into

[26] Jurcut, A. D., Ranaweera, P., & Xu, L. Introduction to IoT Security. 1-39. https://doi.org/10.1002/9781119471509.w5GRef260

[27] Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., & Rehman, S. U. (2023). Cyberattacks and Security of Cloud Computing: A Complete Guideline. Symmetry, 15(11), 1981. https://doi.org/10.3390/sym15111981

[28] World Economic Forum. (2025, June 18). *How energy and manufacturing can stay ahead of cyber threats and protect their tech*. https://www.weforum.org/stories/cybersecurity/cyber-threats-energy-and-manufacturing-ot-technology/

[29] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. (2026). Colonial Pipeline cyber incident. https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

OT consequences even without direct, physical OT manipulation. Under this spectrum, addressing this expanded attack surface requires integrated security frameworks that conceive OT and IT as parts of the same unified ecosystem. Similarly, this requires continuous monitoring, autonomous sensing, and understanding that digital interdependence is now a structural feature of the European energy infrastructure.

Cross-Border Energy Interdependencies

Europe's energy networks are interconnected both in the physical and digital sense. It is a system that requires coordination actions in all its components, the electricity grids, gas pipelines, renewable energy infrastructures, and cross-border interconnectors. Resilience depends largely on said coordinated operations. On the one hand, this continental interdependence improves energy security by having states share resources, collectively check the balance between supply and demand, and – most importantly - respond collectively to disruptions, attacks, and threats. On the other hand though, this interconnection "allows for" systemic exposure[30]. Not only an attack, but also an operational failure in one subsystem can cascade across systems and borders. A cyber intrusion that affects a transmission operator in one country can very quickly, in a matter of minutes, destabilise the neighboring grids.

Also, renewable energy systems are especially vulnerable to disruptions as they rely heavily on forecasting algorithms and automated balancing

[30] Alves, José and Estevão, João, From Fuel Dependence to Network Dependence: Cross-Border Electricity Interdependence and Strategic Vulnerability in Europe's Energy Transition (2026). CESifo Working Paper No. 12836, Available at https://ssrn.com/abstract=7195259

mechanisms. Their dependence on forecasting renders them sensitive vis-à-vis a possible manipulation of forecasting data as this could create imbalances that propagate across all interconnected markets. The European Network of Transmission System Operators for Electricity[31] (ENTSO-E) has highlighted the systemic nature of grid stability[32]. In light of the above, it becomes obvious that regional balancing mechanisms rely heavily on digital forecasting, automated control systems, and on uninterrupted cross-border data flows. Thus, a disruption in one country affects neighbouring countries almost immediately. This chain reaction was evident in several recent cyber intrusions that produced cascading regional effects requiring prompt and effective coordinated response[33].

Coordination is regional and continental - not national - and central for energy resilience. Also, it is complex. Addressing interdependencies across countries, coordinating distinct regulatory frameworks, sharing situational awareness across the operators - all of this requires a high level of joint operational capability[34]. More so, since energy security is inseparable from digital resilience and geopolitical stability. Hybrid perpetrators, exactly because they understand and exploit the strategic value of cross border interdependencies, target vulnerable points where coordination is essential but remains fragile. A

[31] ENTSO-E. (2024).European Resource Adequacy Assessment (ERAA) 2024. Brussels: ENTSO-E. https://www.entsoe.eu/publications/general-publications/annual-report/

[32] See above no 29.

[33] Yu, Xinghuo & Xue, Yusheng. (2016). Smart Grids: A Cyber–Physical Systems Perspective. Proceedings of the IEEE. 104. 1058-1070. 10.1109/JPROC.2015.2503119.

[34] Gökçe, Osman Zeki & Hatipoglu, Emre & Belaïd, Fateh, 2024. "Navigating energy diplomacy in times of recovery and conflict: A study of cross-border energy trade dynamics," Resources Policy, Elsevier, vol. 90(C).

disruption that affects one interconnector, for example, may create political tension between two (or more) states, especially if attribution is doubtful or disputed. To manage these interdependencies effectively requires technical solutions, political commitment, institutional cooperation, and an investment in joint functional exercises across borders.

Case Studies: Cyber-Physical Hybrid Campaigns

Numerous major events have demonstrated how hybrid threats evolve through time and the ways in which they affect energy systems. These cases are not isolated attacks; they represent a modus operandi that hybrid intruders have advanced over time. They demonstrate the strategic rationale that drives cyber-physical operations, and show the vulnerabilities inherent in digitalised energy systems. The attacks on Ukraine's power grid between 2015 and 2022 remain the epitome of cyber-induced blackouts. In 2015, more than two hundred thousand customers were left without power[35], the attackers were tech-savvy enough to manage to disrupt SCADA systems and operational procedures. In 2016, the Industroyer malware exploited IEC 104 protocols to disrupt substations[36]. The 2022 Industroyer2 variant[37], which was deployed during active conflict, targeted high voltage substations with

[35] Whitehead, David & Owens, Kevin & Gammel, Dennis & Smith, Jess. (2017). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. 1-8. 10.1109/CPRE.2017.8090056.

[36] L. Salazar et al., "A Tale of Two Industroyers: It was the Season of Darkness," in 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2024, pp. 312-330, doi: 10.1109/SP54263.2024.00162 at https://www.computer.org/csdl/proceedings-article/sp/2024/313000a162/1Ub24B7070k#:~:text=https%3A//doi.ieeecomputersociety.org/10.1109/SP54263.2024.00162

[37] Ibid.

malware designed to coordinate shutdowns. Malware NotPetya, although it was not designed to target OT systems, caused global disruption through supply chain compromise[38]. NotPetya spread through an accounting software update, and affected companies worldwide. For instance, Maersk, a Danish logistics giant and one of the largest containers shipping companies worldwide, was not only affected by NotPetya, but paralysed. Fuel deliveries were significantly delayed, operations were halted, and energy logistics were disrupted. Rosneft and other energy companies experienced operational disruption[39].

NotPetya proved how an attack on corporate IT systems can impact severely energy supply chains. Similarly, the Colonial Pipeline incident showed how an IT ransomware attack can trigger OT consequences without any direct intrusion into the operational physical infrastructure: the pipeline operator shut down operations as a precaution, leading to fuel shortages, panic buying, and economic disruption across multiple US states[40]. This incident was a testimony of the fragility of energy logistics. It was also a proof that prompt situational awareness is of the utmost importance to avoid escalation and cascading effects. Then, Saudi Aramco's Shamoon attack in 2012 revealed how susceptible to manipulation the corporate IT systems in

[38] Welburn, Jonathan & Strong, Aaron. (2021). Systemic Cyber Risk and Aggregate Impacts. Risk Analysis. 42. 10.1111/risa.13715.

[39] Simos, M. (2018, February 5). Overview of Petya, a rapid cyberattack. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2018/02/05/overview-of-petya-a-rapid-cyberattack/

[40] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. (2026). Colonial Pipeline cyber incident at https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

the energy sector are[41]. Shamoon destroyed tens of thousands of computers and forced manual operations for activities that are easily handled automatically. This disrupted global oil markets. Hence, although OT systems were not directly affected by Shamoon, the attack demonstrated how corporate paralysis can influence energy markets worldwide[42].

Understandably, the Stuxnet malware attack of 2010 remains to this day the most striking example of cyber-physical sabotage. Stuxnet, a sophisticated, tailor-made malware created to infiltrate the PLCs of the Iranian Natanz facilities and sabotage the nuclear centrifuges - which it did, with astonishing success. It manipulated remotely centrifuge speeds, causing massive physical destruction[43]. Stuxnet demonstrated that digital attack can produce kinetic effects, something never seen before then. Collectively, these indicative, well-known cases reveal the diverse and severe impacts malicious hybrid incidents can have on energy supply, grid stability, and critical infrastructure resilience as a whole. They prove that both direct OT sabotage and indirect IT compromise can destabilise our interconnected energy systems.

Regulatory Evolution: From Cybersecurity to Systemic Resilience

The EU regulatory framework has significantly evolved in response to escalating hybrid threats so as to catch up

[41] Alsaeed, Alaa. (2021). The Cyber Attack on Saudi Aramco in 2012. Asian Journal of Engineering and Applied Technology. 10. 25-28. 10.51983/ajeat-2021.10.2.3057.

[42] Albano, K., & Kessem, L. (2022). The full Shamoon: How the devastating malware was inserted into networks. IBM X-Force. https://www.ibm.com/think/x-force/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks

[43] Cybersecurity and Infrastructure Security Agency. (2014, January 8). ICS Advisory ICSA-10-238-01B: Stuxnet malware mitigation (Update B). https://www.cisa.gov/news-events/ics-advisories/icsa-10-238-01b

with the novel modi operandi of perpetrators. The Network and Information Security 2 (NIS2)[44] Directive of 2022 asks for mandatory risk management obligations, prompt incident reporting, and comprehensive supply chain oversight. It further places emphasis on the operators to adopt measures that address the systemic environment of digital risks. The Cyber Resilience Act (CRA) of 2024 introduces a shift towards secure-by-design digital components. It requires tech manufacturers to perform vulnerability management, and it imposes accountability for their insecure software and hardware[45].

This approach recognises that all digital products that are used in energy systems have to be secure throughout their lifecycle. The 2022 Critical Entities Resilience Directive[46] (CERD) focuses on both physical and hybrid resilience, requiring cross-border coordination, business continuity of essential services, and risk assessment pertinent to both the digital and physical domains. The Digital Operational Resilience Act[47] (DORA), although

[44] European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). Official Journal of the European Union.

[45] European Parliament & 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) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*. Official Journal of the European Union at https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng?utm_source=copilot.com

[46] European Parliament & 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. https://eur-lex.europa.eu/eli/dir/2022/2557/oj

[47] European Parliament & Council of the European Union. (2022). *Regulation (EU) 2022/2554 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*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

it pertains to the financial sector, is also relevant for energy finance interdependencies, as energy markets rely heavily on financial systems for their trading and investments. Thus, a disruption in financial systems affects energy operations, and vice versa. Together, all the above-mentioned frameworks form a nexus of resilience, aimed to safeguard the whole cycle: secure operations, secure by design products both hardware and software, resilient critical infrastructure, and safe financial transactions and dependencies.

All these pillars are digitally interconnected, and energy systems are recognised for what they really are: strategic assets needing constant oversight. The EU legal framework's evolution mirrors the shift from cybersecurity of individual components or services, to a comprehensive systemic resilience policy. It reflects the understanding that energy systems are nested in complex digital ecosystems, cross-border interdependencies, and changing geopolitical dynamics. Under this light, resilience now requires effective governance, state-of-the-art technology, security-by-design, risk and crisis management that takes into account these complexities, joint cross-borders exercises, and lifelong learning for operational competence.

Emerging Hybrid Threat Scenarios

Looking ahead, hybrid threats will continue to evolve, as do the ever-shifting geopolitical dynamics and the emerging quantum technologies[48]. Hybrid activity will now involve more sophisticated forms of AI-driven

[48] Elugbadebo, Olabode. (2025). "Quantum computing threats to energy grid security" at https://www.researchgate.net/publication/395524167_quantum_computing_threats_to_energy_grid_security/citation/download

intrusion in OT infrastructure, as Machine Learning models are rapidly analysing industrial processes, and thus, can identify delicate vulnerabilities in grid control systems or renewable energy forecasting[49]. Emerging scenarios pertain to coordinated cyber-physical sabotage of interconnectors[50]. Continental cross-border energy flows rely on specific critical nodes (be it, interconnectors, pipelines, LNG[51] terminals, etc.) If any of them is disrupted - or attacked - this could destabilise the whole region. Also, perpetrators may try to combine digital infiltration with physical sabotage, attacking substations or transmission lines at specific moments when grids are under stress due to adverse weather conditions or even market instabilities.

Manipulation of and interference in renewable energy forecasting systems is also expected to rise, as Europe raises its reliance on wind and solar power. Forecasting precision is becoming, thus, essential for grid stability. A perpetrator who distorts forecasting data without altering them enough to trigger an alarm, could still create imbalances and operational pressure[52]. The emerging hydrogen economy expectedly introduces new vulnerabilities, as hydrogen production, storage, and

[49] Assenza, G., Ortalda, A., & Setola, R. (2024). Redefining systemic cybersecurity risk in interconnected environments. Applied Cybersecurity & Internet Governance, 3(2), 144–169. https://doi.org/10.60097/ACIG/192119

[50] European Union Institute for Security Studies. (2025, August 25). *On a war footing: Securing critical energy infrastructure*. EUISS Brief. https://www.iss.europa.eu/publications/briefs/war-footing-securing-critical-energy-infrastructure

[51] Liquefied Natural Gas.

[52] Ebere, Chuma & Vega, Sol & Leeuwen, Eveline & Mashhoodi, Bardia. (2025). Electricity grid and societal vulnerability interconnection: stakeholder implications and integrated solutions in Europe. Environmental Research Letters https://www.researchgate.net/publication/395375533_Electricity_grid_and_societal_vulnerability_interconnection_stakeholder_implications_and_integrated_solutions_in_Europe/citation/download

distribution are being carried out by digital control systems[53]. For a cyber-criminal, or a hybrid perpetrator, hydrogen infrastructure is an appealing target precisely because it is new and complex, and its security frameworks are not mature. In addition, supply chain risks will remain a major vector, as inverter builders, turbine manufacturers, and sensor providers, all indicate potential entry points for hybrid threats[54].

For example, a non-descript compromised firmware update could impact a broadly used component and create systemic exposure across multiple operators. Finally, disinformation campaigns through social media amplify the impact of technical incidents[55]. Energy prices volatility, long outages, and supply shortages may all be weaponised, and thus, easily politicised. Hybrid perpetrators may instrumentalise social media handles, targeted messaging, and manipulated data to establish public anxiety and, in turn, political pressure[56]. These emerging scenarios highlight the need for integrated resilience policies and targeted measures that combine technical, operational, legal, organisational, and policy approaches. They also highlight the importance of a

[53] Ma, H., Lu, Y., Kou, Z., Xue, Z., Yu, W., Zhang, K., Deng, P., Di, C., Zhu, Y., Wang, H., & Chen, Z. (2025). Cybersecurity and cyber-attacks in the growing natural gas and hydrogen Industry: A systematic review of challenges and opportunities. *Gas Science and Engineering*, *143*, 205744. https://doi.org/10.1016/j.jgsce.2025.205744

[54] HyDelta Consortium. (2026). *Value chain and system development: Hydrogen component manufacturing readiness and spatial requirements (D4c.1 – Supply chain risk management approach for hydrogen infrastructure components)*. HyDelta 3, WP4.3. TKI Nieuw Gas | Topsector Energie, Project TKI2023-HyDelta. Zenodo.

[55] Barnard, Stephen. (2024). Hacking Hybrid Media: Power and Practice in an Age of Manipulation. 10.1093/oso/9780197570272.001.0001.

[56] European Commission, Joint Research Centre. (2023). *Fortifying defence: Strengthening critical energy infrastructure against hybrid threats*. Directorate E – Space, Security and Migration, Unit JRC.E.2 Technologies for Space, Security and Connectivity. EU Science Hub. https://joint-research-centre.ec.europa.eu

novel technological capability: systems with autonomous sensing, rapid situational awareness, and cross-border coordination[57].

UAVs and Autonomous Systems as Resilience Enablers

Autonomous aerial systems, also known as Unmanned Aerial Vehicles (UAVs), or drones, are becoming increasingly important for enhancing energy infrastructure protection and resilience[58]. Their contribution pertains not only in their ability to inspect physical assets even in harsh weather or adverse geological/environmental conditions but also in their capacity to provide real-time situational awareness during a hybrid disruption. Their central advantage is that they can operate in environments that are unreachable, hazardous, or time-consuming for human teams[59]. They can detect promptly and efficiently anomalies such as thermal irregularities, electromagnetic disturbances, physical sabotage, and also jamming or spoofing (albeit, being themselves targets of both jamming[60] and spoofing[61]). This is a beneficial capability in OT environments, as early detection potentially prevents massive cascading effects.

[57] Rangwala, S. (2026, July 9). *Robotics, drones & AI for monitoring energy infrastructure*. Forbes. https://www.forbes.com/sites/sabbirrangwala/2026/07/09/robotics-drones--ai-for-monitoring-energy-infrastructure/

[58] European Commission. (2026). *Communication from the Commission to the European Parliament and the Council: Action plan on drone and counter-drone security (COM/2026/81 final)*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026DC0081

[59] European Union Aviation Safety Agency. (2026). Civil drones. https://www.easa.europa.eu/en/domains/civil-drones

[60] Jamming refers to the deliberate interference with a UAV's communication or navigation signals by overwhelming them with noise or competing radio transmissions.

[61] Spoofing means that the attacker forges false signals (e.g., coordinates) that the UAV deems correct.

UAVs also improve cross-border situational awareness, an attribute that is essential in the energy domain, as energy systems are not confined within national boundaries, and disruptions require a coordinated response across different countries. To that end, UAVs offer shared data feeds into a crisis cell (an emergency team of experts) which assist operators in their rapid understanding of the magnitude and nature of an incident[62].

The EU-funded SPEAR[63] project showcases new, innovative technologies in drones and robotics, designed through Artificial Intelligence to "think" autonomously, address capability gaps of today in critical infrastructure protection, and provide real time communication with crisis centres, independent sensing and decision making, and swift post-incident assessment. They verify the existence and degree of physical damage, assess the condition of nodes, and support restoration. Most importantly, their autonomous operation minimises the burden on human teams. Furthermore, UAVs assist in communication during a crisis, as they deliver live video feeds, mapping data, and visual information that can be shared with operators, regulators, and emergency services, enhancing their coordination at a moment that is central for accurate public communication, maintaining trust with citizens, and preventing societal panic[64]. Considering all of the above, and in the broader context of systemic resilience, UAVs represent another

[62] Pal, Osim & Shovon, Md & Ph. D., M. & Shin, Jungpil. (2024). In-depth review of AI-enabled unmanned aerial vehicles: trends, vision, and challenges. Discover Artificial Intelligence. 4. 10.1007/s44163-024-00209-1.
[63] https://www.spear-robotics.com/
[64] Zobel, J., & Landsberg, L. (2025). *Future communication applications of UAVs for increased resilience of command and control systems*. In *Proceedings of the 22nd ISCRAM Conference: Visions for Future Crisis Management* (WiP Paper). Halifax, Canada.

operational instrument in Europe's approach vis-à-vis energy infrastructure protection.

They are a useful technology in our resilience toolbox, functioning most effectively as an added, integrated layer within a multi-layered protection system. Nevertheless, while they provide an advantage in real-time situational awareness, they cannot constitute a standalone panacea for our systemic cyber-physical infrastructure vulnerabilities. Rather, their efficacy is at times dependent upon the distinct technological limitations inherent to current UAV platforms[65] (i.e., limited battery life affecting prolonged flying, possible degradation of sensor accuracy in adverse meteorological conditions, their own exposure to electronic warfare[66], etc.). Consequently, autonomous systems are important in complementing traditional deep-defense mechanisms like network segmentation and cryptographic hardware authentication, albeit not sufficient on their own.

Policy Implications

Evidently, in light of the aforementioned, strengthening Europe's energy infrastructure resilience requires a combination of governance, technology, and coordinated operational capability. The regulatory frameworks cited above, all introduced in recent years, are sine qua non steppingstones towards systemic resilience in the energy sector. Yet, regulation alone

[65] Pal, O., Shovon, M., & Shin, J. (2024). In-depth review of AI-enabled unmanned aerial vehicles: trends, vision, and challenges. Discover Artificial Intelligence, 4, 1-22, doi.org
[66] As Above n. 58

cannot address the complexity of hybrid threats, as perpetrators are early technology adopters, and consequently always one step ahead[67]. To mitigate that, continuous monitoring of critical nodes is of the utmost importance.

While the EU regulatory framework (specifically the NIS2 and CER Directives) already mandates said continuous monitoring for critical entities, an urgent need for granular, sector-specific technical standards still remains in order to enforce this mandate effectively across the OT infrastructure nodes, such as hydrogen sensors and power inverters, which to this day remain exposed to sophisticated hybrid attacks[68]. As we have seen, energy operators need visibility into both their digital and physical environments at all times. Hence, the most technologically advanced anomaly detection systems should be integrated into the NIS2 obligations[69]. An EU-wide platform for hybrid threat early warning would enhance cross-border coordination and in turn prompt response. Such a platform could integrate data streams from UAVs, sensors, and digital monitoring systems, while supporting crisis management and decision-making during hybrid disruptions. Although the EU Cyber Resilience Act enforces 'secure-by-design' mandates and lifecycle vulnerability management, its

[67] Spagnuolo, G. (2026). *The cognitive battlefield of hybrid warfare*. NATO Defense College Foundation.

[68] Nitzsche, T. (2025, July 24). *NIS2 gives Europe's hydrogen sector a head start on cybersecurity*. H2 View. Reprinted as External Blog, ABB Energy Industries (2025, August 18). https://new.abb.com/news/detail/128344/nis2-gives-europes-hydrogen-sector-a-head-start-on-cybersecurity

[69] Agency for the Cooperation of Energy Regulators. (2025, June 13). ACER issues a guide on benchmarking cybersecurity investments in the EU electricity sector. https://www.acer.europa.eu/news/acer-issues-guide-benchmarking-cybersecurity-investments-eu-electricity-sector

enforcement is deferred until the end of 2027, leaving open a window of hybrid opportunity. Additionally, the Act's lack of a retroactive framework leaves the older, legacy OT nodes unprotected for the time being which highlights the necessity for immediate measures like autonomous aerial sensing[70].

Another (hard to quickly accomplish) goal is the standardisation of OT security requirements across operators in different states[71]. Different energy companies reach different levels of maturity in their OT security guidelines, which creates uneven exposure. Harmonised standards would at least guarantee a lowest common denominator of security, upon which we could build further. Expanding ENISA's systemic risk management mandate would further uphold optimal supervision of cross border interdependencies. To that effect, ENISA could produce models to simulate cascading failures so as to contribute in building a shared stance in risk and crisis management among the operators in the different states[72]. Furthermore, cross-border UAV response teams could be funded under the Energy and Home Directorates. These teams would establish real-time situational awareness during a hybrid disruption, and advance prompt coordination. Finally, incident reporting guidelines and protocols should be

[70] Wirtek (2025). *What the Cyber Resilience Act requires of connected products*. Wirtek Blog. https://www.wirtek.com/blog/what-the-cyber-resilience-act-requires-of-connected-products

[71] ShieldWorkz. (2025, October 27). *A guide to OT security for the renewable energy sector*. ShieldWorkz Blog. https://shieldworkz.com/blogs/a-guide-to-ot-security-for-the-renewable-energy-sector

[72] EPIS Think Tank. (2025). *Cyberattacks on EU critical infrastructure: Scale, scope, and sectoral threat trends (2024–2025).* EPIS. https://epis-thinktank.com/publications/cyberattacks-on-eu-critical-infrastructure

harmonised across the EU Member States[73], as maintaining consistency in reporting shall create a culture of shared awareness, improve data accuracy, and uphold collaboration.

Future Research Directions

Future research needs to study quantitative modelling of cascading failures in interconnected energy systems, as such models help us understand how disruptions propagate, and identify entry points[74] where intervention could prevent escalation. The role of AI-enabled offensive cyber capabilities targeting OT environments warrants further examination[75]. Perpetrators increasingly utilise machine learning models either to automate reconnaissance, or to pinpoint vulnerabilities. Effective countermeasures will come about from comparative studies of UAV deployments across the EU, so that best practices can be quickly derived and used as actionable insights. These studies could examine how different operators across the Member States integrate UAVs into their monitoring systems, their early-warning platforms, and their incident response frameworks. Finally, the relatively recent digitalisation

[73] Ebert, N., Schaltegger, T., Ambuehl, B., Geppert, T., Trammell, A., Knieps, M., & Zimmermann, V. (2025). *Learning from safety science: designing incident reporting systems in cybersecurity.* Journal of Cybersecurity, 11(1), tyaf019.

[74] Zhong, Wanqing & Rasouli, Sina & Singh, Atul Kumar & Mohandes, Saeed Reza & Antwi-Afari, Maxwell & Cheung, Clara & Manu, Patrick & Agrawal, Unnati. (2025). The Adoption of UAVs for Enhancing Safety in Construction Industry: A Systematic Literature Review. Intelligent Infrastructure and Construction. 1. 3. 10.3390/iic1010003.

[75] Joshi, Amit & Spilbergs, Aivars & Mikelsone, Elina. (2024). AI-enabled drone autonomous navigation and decision making for defence security, environment, technology, resources. Proceedings of the International Scientific and Practical Conference. 4. 138-143. 10.17770/etr2024vol4.8237.

of the hydrogen economy[76] also hosts new exposures that require further study, as hydrogen infrastructure relies heavily on digital control systems, and its security frameworks are not yet mature. Therefore, research should examine how hybrid actors might target hydrogen infrastructure and how their resilience can be strengthened.

Conclusion

Digital interdependence has massively transformed Europe's energy systems into strategic assets, whose vulnerabilities can be exploited by hybrid criminals. Perpetrators target complexity, interconnections, and timing, producing disruptions that carry (geo)political, economic, and societal consequences. Traditional cybersecurity approaches are insufficient against such multidomain threats. Resilience requires continuous monitoring, secure-by-design digital components, cross-border coordination frameworks, systemic risk modelling, and advanced situational awareness. Autonomous aerial systems provide an additional operational capacity that Europe's energy security frameworks can benefit from. They can be a cog in the "resilience machine" that tackles systemic fragility and assists in of our wider, multi-layered defensive matrix tasked with mitigating European energy vulnerability.

Policymakers should (continue to) treat the energy grid as an active geopolitical front line, that demands tightly integrated governance backed by autonomous tactical tools, so that our systems remain resilient to targeted hybrid coercion. Ultimately, defending Europe's energy

[76] International Energy Agency. (2023). Power systems in transition: Cyber resilience. https://www.iea.org/reports/power-systems-in-transition/cyber-resilience

grids requires moving past the purely reactive, checkbox security guidelines and standard operating procedures, to embrace new technologies and a multi-domain approach before perpetrators do.

Literature:

1. Agency for the Cooperation of Energy Regulators. (2025, June 13). ACER issues a guide on benchmarking cybersecurity investments in the EU electricity sector. https://www.acer.europa.eu/news/acer-issues-guide-benchmarking-cybersecurity-investments-eu-electricity-sector
2. Agency for the Cooperation of Energy Regulators. (2026). Cybersecurity network code for electricity. https://www.acer.europa.eu/electricity/cybersecurity
3. Albano, K., & Kessem, L. (2022). The full Shamoon: How the devastating malware was inserted into networks. IBM X-Force. https://www.ibm.com/think/x-force/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks
4. Alsaeed, Alaa. (2021). The Cyber Attack on Saudi Aramco in 2012. Asian Journal of Engineering and Applied Technology. 10. 25-28. 10.51983/ajeat-2021.10.2.3057.
5. Alves, J., & Estevão, J. (2026). From Fuel Dependence to Network Dependence: Cross-Border Electricity Interdependence and Strategic Vulnerability in Europe's Energy Transition (CESifo Working Paper No. 12836). CESifo. Available at EconPapers: repec.org CESifo Working Paper No. 12836, Available at SSRN: https://ssrn.com/abstract=7195259
6. Assenza, G., Ortalda, A., & Setola, R. (2024). Redefining systemic cybersecurity risk in interconnected environments. Applied Cybersecurity & Internet Governance, 3(2), 144–169. https://doi.org/10.60097/ACIG/192119
7. Barnard, Stephen. (2024). Hacking Hybrid Media: Power and Practice in an Age of Manipulation. 10.1093/oso/9780197570272.001.0001.
8. Brännlund, A., & Peterson, L. (2024). Power politics: How electric grievances shape election outcomes. Ecological Economics, 217, 108077. https://doi.org/10.1016/j.ecolecon.2023.108077

9. Council of the European Union. (2026). Hybrid threats. https://www.consilium.europa.eu/en/policies/hybrid-threats/

10. Cybersecurity and Infrastructure Security Agency. (2014, January 8). ICS Advisory ICSA-10-238-01B: Stuxnet malware mitigation (Update B). https://www.cisa.gov/news-events/ics-advisories/icsa-10-238-01b

11. Cybersecurity and Infrastructure Security Agency. (2026). Energy sector: Critical infrastructure security and resilience. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector

12. Data Breach Registries & Monitoring Services, Have I Been Pwned. (2025, September). Data breach registry: Miljödata https://haveibeenpwned.com/Breach/Miljodata

13. Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., & Rehman, S. U. (2023). Cyberattacks and Security of Cloud Computing: A Complete Guideline. Symmetry, 15(11), 1981. https://doi.org/10.3390/sym15111981

14. DIESEC. (2025, October 29). Ransomware in the supply chain: Swedish IT supplier gets hit. https://diesec.com/2025/10/ransomware-in-the-supply-chain-swedish-it-supplier-gets-hit/

15. Digital Intrusion and Critical Infrastructure Cyber-Attacks, Brantly, A. F. (2021). The cyber-physical nexus: Assessing risks to critical infrastructure. Journal of Cyber Policy, *6*(2), 184–202. https://doi.org/10.1080/23738871.2021.1983572

16. Ebere, Chuma & Vega, Sol & Leeuwen, Eveline & Mashhoodi, Bardia. (2025). Electricity grid and societal vulnerability interconnection: stakeholder implications and integrated solutions in Europe. Environmental Research Letters https://www.researchgate.net/publication/395375533_Electricity_grid_and_societal_vulnerability_interconnection_stakeholder_implications_and_integrated_solutions_in_Europe/citation/download

17. Ebert, N., Schaltegger, T., Ambuehl, B., Geppert, T., Trammell, A., Knieps, M., & Zimmermann, V. (2025). Learning from safety science: designing incident reporting systems in cybersecurity. Journal of Cybersecurity, 11(1), tyaf019.

18. Elugbadebo, Olabode. (2025). “Quantum computing threats to energy grid security” at https://www.researchgate.net/publication/395524167_quantum_computing_threats_to_energy_grid_security/citation/download

19. ENTSO-E. (2024).European Resource Adequacy Assessment (ERAA) 2024. Brussels: ENTSO-E. https://www.entsoe.eu/publications/general-publications/annual-report/
20. EPIS Think Tank. (2025). Cyberattacks on EU critical infrastructure: Scale, scope, and sectoral threat trends (2024–2025). EPIS. https://epis-thinktank.com/publications/cyberattacks-on-eu-critical-infrastructure
21. European Commission, Directorate-General for Communications Networks, Content and Technology. (2026). NIS2 Directive: Securing network and information systems. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
22. European Commission, Joint Research Centre. (2023). Fortifying defence: Strengthening critical energy infrastructure against hybrid threats. Directorate E – Space, Security and Migration, Unit JRC.E.2 Technologies for Space, Security and Connectivity. EU Science Hub. https://joint-research-centre.ec.europa.eu
23. European Commission. (2026). Communication from the Commission to the European Parliament and the Council: Action plan on drone and counter drone security (COM/2026/81 final). EUR Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026DC0081
24. European Commission. (2026). Communication from the Commission to the European Parliament and the Council: Action plan on drone and counter drone security (COM/2026/81 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026DC0081
25. European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). Official Journal of the European Union.
26. European Parliament & 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. https://eur-lex.europa.eu/eli/dir/2022/2557/oj
27. European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2554 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. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

28. European Parliament & 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) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Official Journal of the European Union at https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng?utm_source=copilot.com

29. European Union Agency for Cybersecurity. (2025, October ENISA) Threat Landscape. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

30. European Union Aviation Safety Agency. (2026). Civil drones. https://www.easa.europa.eu/en/domains/civil-drones

31. European Union Institute for Security Studies. (2025, August 25). On a war footing: Securing critical energy infrastructure. EUISS Brief. https://www.iss.europa.eu/publications/briefs/war-footing-securing-critical-energy-infrastructure

32. Freitag, Nils, The Political Consequences of Energy Price Shocks: Evidence from Berlin, July 01, 2026. Available at SSRN: https://ssrn.com/abstract=7165539 or http://dx.doi.org/10.2139/ssrn.7165539

33. Galeotti, M. (2023). The weaponisation of everything: A field guide to the new way of war. Yale University Press. https://yalebooks.yale.edu/book/9780300270419/the-weaponisation-of-everything/

34. Gökçe, Osman Zeki & Hatipoglu, Emre & Belaïd, Fateh, 2024. "Navigating energy diplomacy in times of recovery and conflict: A study of cross-border energy trade dynamics," Resources Policy, Elsevier, vol. 90(C).

35. Goldthau, A., Keim, M., & Westphal, K. (2018). The geopolitics of energy transformation: governing the shift: transformation dividends, systemic risks and new uncertainties. (SWP Comment, 42/2018). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. https://nbn-resolving.org/ urn:nbn:de:0168-ssoar-60135-0

36. Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies
37. https://doi.org/10.1080/23738871.2021.1983572
38. Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats, & European Commission's Joint Research Centre (JRC). (2021). The landscape of hybrid threats: A conceptual model. Publications Office of the European Union.
39. HyDelta Consortium. (2026). Value chain and system development: Hydrogen component manufacturing readiness and spatial requirements (D4c.1 – Supply chain risk management approach for hydrogen infrastructure components). HyDelta 3, WP4.3. TKI Nieuw Gas | Topsector Energie, Project TKI2023 HyDelta. Zenodo.
40. International Energy Agency. (2023). Power systems in transition: Cyber resilience. https://www.iea.org/reports/power-systems-in-transition/cyber-resilience.
41. International Energy Agency. (2025). Energy and AI: World Energy Outlook special report. https://iea.blob.core.windows.net/assets/de9dea13-b07d-42c5-a398-d1b3ae17d866/EnergyandAI.pdf
42. Joshi, Amit & Spilbergs, Aivars & Mikelsone, Elina. (2024). AI-enabled drone autonomous navigation and decision making for defence security, environment, technology, resources. Proceedings of the International Scientific and Practical Conference. 4. 138-143. 10.17770/etr2024vol4.8237.
43. Jurcut, A. D., Ranaweera, P., & Xu, L. Introduction to IoT Security. 1-39. https://doi.org/10.1002/9781119471509.w5GRef260
44. L. Salazar et al., "A Tale of Two Industroyers: It was the Season of Darkness," in 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2024, pp. 312-330, doi: 10.1109/SP54263.2024.00162 at https://www.computer.org/csdl/proceedings-article/sp/2024/313000a162/1Ub24B7070k#:~:text=https%3A//doi.ieeecomputersociety.org/10.1109/SP54263.2024.00162
45. Ma, H., Lu, Y., Kou, Z., Xue, Z., Yu, W., Zhang, K., Deng, P., Di, C., Zhu, Y., Wang, H., & Chen, Z. (2025). Cybersecurity and cyber-attacks in the growing natural gas and hydrogen Industry: A systematic review of challenges and opportunities. Gas Science and Engineering, 143, 205744. https://doi.org/10.1016/j.jgsce.2025.205744

46. NATO. (2026, January 29). Countering hybrid threats. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

47. Nitzsche, T. (2025, July 24). NIS2 gives Europe's hydrogen sector a head start on cybersecurity. H2 View. Reprinted as External Blog, ABB Energy Industries (2025, August 18). https://new.abb.com/news/detail/128344/nis2-gives-europes-hydrogen-sector-a-head-start-on-cybersecurity

48. Pal, Osim & Shovon, Md & Ph. D., M. & Shin, Jungpil. (2024). In-depth review of AI-enabled unmanned aerial vehicles: trends, vision, and challenges. Discover Artificial Intelligence. 4. 10.1007/s44163-024-00209-1.

49. Rangwala, S. (2026, July 9). Robotics, drones & AI for monitoring energy infrastructure. Forbes. https://www.forbes.com/sites/sabbirrangwala/2026/07/09/robotics-drones--ai-for-monitoring-energy-infrastructure/

50. Rubin, G. J., & Rogers, M. B. (2019). Behavioural and psychological responses of the public during a major power outage: A literature review. International Journal of Disaster Risk Reduction, 38, 101226. https://doi.org/10.1016/j.ijdrr.2019.101226

51. Sectech Solutions. (2024, September 3). The intersection of OT and IT security in the energy sector. https://www.sectechsolutions.co.uk/post/the-intersection-of-ot-and-it-security-in-the-energy-sector

52. ShieldWorkz. (2025, October 27). A guide to OT security for the renewable energy sector. ShieldWorkz Blog. https://shieldworkz.com/blogs/a-guide-to-ot-security-for-the-renewable-energy-sector

53. Simos, M. (2018, February 5). Overview of Petya, a rapid cyberattack. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2018/02/05/overview-of-petya-a-rapid-cyberattack/

54. Spagnuolo, G. (2026). The cognitive battlefield of hybrid warfare. NATO Defense College Foundation.

55. SPEAR Project at https://www.spear-robotics.com/

56. Strojny, J., & Kacorzyk, P. (2025). Economic Aspects of Energy Production, Distribution and Consumption. Energies, 18(6), 1369. https://doi.org/10.3390/en18061369

57. U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. (2026). Colonial

Pipeline cyber incident. https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

58. Wang, Q., Ren, F., & Li, R. (2024). Geopolitics and energy security: A comprehensive exploration of evolution, collaborations, and future directions. Humanities and Social Sciences Communications, 11(1), 1071. https://doi.org/10.1057/s41599-024-03507-2

59. Welburn, Jonathan & Strong, Aaron. (2021). Systemic Cyber Risk and Aggregate Impacts. Risk Analysis. 42. 10.1111/risa.13715.

60. Whitehead, David & Owens, Kevin & Gammel, Dennis & Smith, Jess. (2017). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. 1-8. 10.1109/CPRE.2017.8090056.

61. Wirtek (2025). What the Cyber Resilience Act requires of connected products. Wirtek Blog. https://www.wirtek.com/blog/what-the-cyber-resilience-act-requires-of-connected-products

62. World Economic Forum. (2025, June 18). How energy and manufacturing can stay ahead of cyber threats and protect their tech. https://www.weforum.org/stories/cybersecurity/cyber-threats-energy-and-manufacturing-ot-technology/

63. Yu, Xinghuo & Xue, Yusheng. (2016). Smart Grids: A Cyber–Physical Systems Perspective. Proceedings of the IEEE. 104. 1058-1070. 10.1109/JPROC.2015.2503119.

64. Zhong, Wanqing & Rasouli, Sina & Singh, Atul Kumar & Mohandes, Saeed Reza & Antwi-Afari, Maxwell & Cheung, Clara & Manu, Patrick & Agrawal, Unnati. (2025). The Adoption of UAVs for Enhancing Safety in Construction Industry: A Systematic Literature Review. Intelligent Infrastructure and Construction. 1. 3. 10.3390/iic1010003.

65. Zobel, J., & Landsberg, L. (2025). Future communication applications of UAVs for increased resilience of command and control systems. In Proceedings of the 22nd ISCRAM Conference: Visions for Future Crisis Management (WiP Paper). Halifax, Canada.

CC BY NC ND