SECURITY & DEFENCE QUARTERLY

Weaponised interdependence and European energy security: Infrastructure, systemic vulnerability, and the post-2022 transformation

Elmir Badalov

elmir.badalov@khazar.org

https://orcid.org/0000-0003-3858-9079

School of Humanities, Education and Social Sciences, Khazar University, 41 Mehseti Str., AZ 1096, Baku, Azerbaijan

Abstract

This article extends a concept developed by Farrell and Newman (2019) beyond its original financial and digital domains to physical energy infrastructure, examining how the Russia–Ukraine war has transformed European energy security from a market-based relationship into a condition of systemic vulnerability. The analysis employs qualitative document analysis of publicly available European Union's policy instruments, International Energy Agency's market reports, and European Union Agency for Cybersecurity's threat assessments, structured around a three-domain framework encompassing physical infrastructure, digital systems, and governance arrangements. Diversification strategies implemented after 2022 reduced dependence on Russian energy but simultaneously reconfigured systemic vulnerability across all three domains: liquified natural gas (LNG) import concentration and deployment of floating storage and regasification units created new physical chokepoints; supervisory control and data acquisition and digital vendor dependencies introduced persistent digital interdependencies; and governance fragmentation among member states amplified vulnerability by producing uneven resilience across interconnected systems. European energy security must be reconceptualised as the management of systemic interdependence across interconnected physical, digital, and institutional domains. The article introduces the concept of structural weaponisation potential—the proposition that networked energy systems generate vulnerability as an emergent property of their architecture, independent of any actor's intention to exploit it.

Keywords:

systemic vulnerability, energy infrastructure, Russia–Ukraine war, weaponised interdependence, European energy security

Article info
Received: 18 May 2025
Revised: 18 July 2026
Accepted: 24 July 2026
Available online: 28 August 2026

Citation: Badalov, E. (2026) 'Weaponised interdependence and European energy security: Infrastructure, systemic vulnerability, and the post-2022 transformation', *Security and Defence Quarterly*, 55(3). doi: 10.35467/sdq/226337

Introduction

Russia's full-scale invasion of Ukraine in February 2022 shattered an assumption that had anchored European energy policy for decades: that commercial interdependence with Moscow was, on balance, stabilising. For decades, European Union (EU)–Russia energy relations had been interpreted through the lens of liberal interdependence. On this view, dense economic linkages raise the mutual costs of coercion and thereby discourage it (Keohane and Nye, 1977). Within that framework, integrating Russian hydrocarbons into European markets appeared both rational and prudent (Goldthau and Sitter, 2015). By the early 2020s, Russia supplied approximately 40% of the EU's total natural gas imports through a pipeline network with combined annual capacity exceeding 150 billion (bn) cubic metres (bcm) (International Energy Agency [IEA], 2023). The relationship was deeply embedded. That embeddedness shaped the evolution of European energy governance in ways whose consequences are still being worked through.

The events of 2022 exposed the limitations of that assumption rapidly. Russian gas exports to the EU declined from roughly 155 bcm in 2021 to approximately 27 bcm in 2023—a reduction exceeding 82% in 2 years (IEA, 2023). The sabotage of Nord Stream 1 and Nord Stream 2 in September 2022 destroyed infrastructure representing a combined annual capacity of roughly 110 bcm. It underscored the physical vulnerability of critical energy systems to both political manipulation and outright destruction (Siddi, 2023). Wholesale gas prices at the Dutch Title Transfer Facility (TTF) hub surged to approximately €340 per megawatt-hour (MW-h) in August 2022. The shock cascaded through industrial production, household energy costs, and public finances (IEA, 2023; Sgaravatti *et al.*, 2023b). The EU responded with the REPowerEU strategy, expanding liquified natural gas (LNG) imports and deploying floating storage and regasification units with notable speed. These were genuine achievements. However, they also revealed a structural condition that the diversification narrative tends to obscure.

The existing scholarship has examined this transformation primarily through the lenses of supply diversification, market adjustment, and geopolitics (Goldthau and Sitter, 2022; Kuzemko *et al.*, 2022; Siddi, 2023). The literature remains predominantly supply-centric, paying limited attention to how interdependence itself—embedded in infrastructure networks, digital systems, and governance arrangements—generates systemic vulnerability that persists regardless of supplier identity. This article addresses that gap by applying and extending the concept of weaponised interdependence (Farrell and Newman, 2019) to European energy systems after 2022. The analysis is guided by an explicit research question: How did the diversification strategies adopted after 2022 reconfigure, rather than eliminate, the systemic vulnerability embedded in the physical, digital, and governance domains of European energy systems?

In answering this question, the article advances three arguments. First, pre-2022 European energy governance systematically underestimated systemic and infrastructural risks by prioritising market efficiency over resilience. Second, diversification strategies reduced Russian energy dependence but simultaneously reconfigured vulnerability—through exposure to global LNG markets, new infrastructural chokepoints, digital interdependencies, and the emerging critical minerals dimension of the energy transition. Third, European energy security must be reconceptualised as the capacity to manage systemic interdependence across interconnected physical, digital, and institutional domains. The article proceeds as follows: Section 2 reviews the literature and develops the theoretical framework; Section 3 describes the methodology; Section 4 presents the empirical analysis across three domains; Section 5 discusses the findings; and Section 6 concludes.

Literature review and theoretical framework

Classical accounts of interdependence treat it as a condition generating both sensitivity and vulnerability, but expect its overall effect to be stabilising—the mutual costs of disruption discourage coercion (Keohane and Nye, 1977). This perspective deeply influenced post-Cold War interpretations of EU–Russia energy relations. Yergin (2006) and Goldthau and Sitter (2015) argued that long-term contracts, large-scale infrastructure investments, and regulatory integration created a relatively stable energy relationship. European policy reflected this assumption, prioritising market liberalisation over strategic insulation (European Commission, 2014). Yet even within the liberal framework, Baldwin (1980) established that interdependence does not produce symmetric distributions of power: vulnerability falls unevenly, and structurally advantaged actors can exercise coercive leverage. The 2006 and 2009 Russia–Ukraine gas disputes made this point empirically, but policy responses remained incremental.

Post-2022 scholarship has advanced important insights. Goldthau and Sitter (2022) document how Russia's weaponisation of energy has undermined the liberal market model that long underpinned the EU energy governance, prompting a turn towards more strategic and interventionist policy. Siddi (2023) provides a comprehensive overview of the post-invasion energy landscape. Kuzemko *et al.* (2022) situate the crisis within sustainable energy transformation debates. These contributions are valuable, but they remain predominantly supply-side in orientation. They address who supplies and what is diversified rather than how the structure of interconnected systems—irrespective of supplier identity—shapes the distribution of vulnerability.

The insight that vulnerability and leverage are properties of network structure, rather than of supplier identity alone, is also well established in scholarship produced outside the transatlantic core. Chinese debates on energy security have long treated supply security as inseparable from transit routes and infrastructural exposure, framing dependence on maritime chokepoints as a strategic vulnerability in its own right (Zha, 2006). Similarly, scholarship on Gulf LNG emphasises how an exporter's position within shipping lanes, contract structures, and regional market arrangements conditions its leverage, as Qatar's reorientation towards East Asian markets illustrates (Wright, 2017). Work on Eurasian transit chains shows that the material properties of fuels and the infrastructures that move them shape who holds leverage at each link of the value chain (Balmaceda, 2021). These writings converge on the structural intuition that this article develops.

Farrell and Newman (2019) provide the missing conceptual instrument. Their concept of weaponised interdependence shows how global economic networks can be exploited as instruments of coercion. Two mechanisms are central: the chokepoint effect, which allows actors controlling critical infrastructure nodes to restrict access; and the panopticon effect, which enables surveillance and information control through dominant network positions. Originally formulated for financial and digital networks, the framework has since been extended. Drezner (2021) notes that network structures constrain weaponisers as well as targets; the framework nonetheless identifies structural potential rather than deterministic outcomes—latent leverage that political conditions may or may not activate (Farrell and Newman, 2019, 2023). Farrell and Newman (2023) have themselves traced the framework's operation through the physical plumbing of the world economy, from fibre-optic cables to payment infrastructures, indicating that its mechanisms are not confined to intangible networks and supporting extension to physical energy infrastructure.

This article extends weaponised interdependence through a three-domain analytical model. The first domain is physical infrastructure: pipelines, LNG terminals, floating

storage and regasification units (FSRUs), interconnectors, and subsea cables that form the material backbone of energy flow. This domain exhibits geographic fixity, high capital intensity, and long investment horizons—properties that produce path dependencies and slow adaptation. The second domain is digital systems: supervisory control and data acquisition (SCADA) control systems, smart grid technologies, algorithmic trading platforms, and data analytical tools that manage and optimise physical energy flows. Digital systems introduce cybersecurity vulnerabilities and vendor dependencies that generate forms of interdependence often invisible to supply-side analysis. The third domain is governance: the regulatory frameworks, market institutions, and multi-level coordination mechanisms that shape how energy systems operate and how vulnerability is distributed. Governance asymmetries among member states—particularly in fiscal capacity and regulatory maturity—amplify systemic risk by producing uneven resilience across interconnected systems. The chokepoint and panopticon effects operate across all three domains simultaneously, producing interaction effects that neither domain-specific nor supply-centric analyses capture.

Methods

The analysis employs qualitative document analysis, appropriate to research questions concerning the institutional and regulatory evolution of energy security and the mechanisms of systemic vulnerability. The source corpus is built from three categories: (1) primary EU instruments, which include the REPowerEU Plan (COM(2022) 230 final; European Commission, 2022), Council Regulation (EU) 2022/1369 on demand reduction, Council Regulation (EU) 2022/1032 on gas storage, and the European energy security strategy (COM(2014) 330 final; European Commission, 2014) as the pre-crisis baseline; (2) secondary statistical sources, principally the IEA's (2022, 2023) gas market reports and the European Union Agency for Cybersecurity's (ENISA, 2023) threat landscape; and (3) scholarly literature from peer-reviewed journals indexed in Scopus and Web of Science.

Three procedural clarifications specify how the corpus was assembled and analysed. First, scholarly literature was identified through keyword searches in Scopus and Web of Science ("weaponised interdependence," "energy security," "EU energy governance," and "critical raw materials"), supplemented by citation chaining from Farrell and Newman (2019). Inclusion required peer-reviewed status, publication in English, and direct relevance to at least one of the three domains; purely technical engineering studies were excluded. Second, documents were analysed following the procedure described by Bowen (2009) for qualitative document analysis: an initial skimming pass to establish relevance, a close reading pass, and an interpretive pass in which passages were coded against the three domains. Evidence was assigned to the physical domain, where it concerned material infrastructure, fuels, or physical flows; to the digital domain, where it concerned control systems, software dependencies, or cyber incidents; and to the governance domain, where it concerned regulatory, fiscal, or institutional arrangements. Passages implicating more than one domain were logged as cross-domain interactions and analysed separately, because such interactions are central to the argument. Third, the same three questions were posed of each domain—what latent vulnerability existed before 2022, how chokepoint or panopticon effects were activated during the crisis, and how post-2022 responses reconfigured vulnerability—so that the three domains are examined in a structured and directly comparable manner.

The analytical approach is interpretive rather than explanatory—the goal is to reconstruct the structural logic of systemic vulnerability, not to measure causal weights across

domains. Three limitations apply: the reliance on publicly available documents excludes informal negotiation dynamics; the EU-as-collective-actor framing simplifies significant member-state variation; and the timeframe—2014 to early 2025—captures the acute crisis and its immediate institutional response but not longer-term structural adjustments still underway.

Results

Table 1 summarises the indicators developed in the sections that follow, comparing the pre-2022 configuration of vulnerability with its post-2022 reconfiguration across the three domains and the emerging critical minerals dimension.

Pre-2022 latent vulnerabilities

Prior to 2022, the EU's energy system was characterised by a dense and highly integrated network of cross-border infrastructure, long-term contractual arrangements, and regulatory coordination that placed Russian hydrocarbons at the centre of the European energy mix. Natural gas occupied a particularly central role. By the late 2010s, Russia had become the EU's largest external gas supplier, accounting for roughly 40% of the total imports—approximately 155 bcm annually by 2021 (IEA, 2023). These flows were delivered through an extensive pipeline network: the Brotherhood pipeline through Ukraine (capacity approximately 140 bcm), the Yamal-Europe pipeline via Belarus and Poland (approximately 33 bcm), and the Nord Stream system (Nord Stream 1 at 55 bcm, with Nord Stream 2 adding a further 55 bcm of planned capacity).

These pipelines formed the backbone of a networked system of interdependence linking producers, transit states, and consumers across multiple jurisdictions. Their operation was supported by long-term contracts—often incorporating take-or-pay clauses spanning 20–30 years—that stabilised supply relationships over extended periods (Goldthau and Sitter, 2015). From a network perspective, such arrangements created durable connectivity patterns that reduced short-term volatility but simultaneously increased structural rigidity. Dependence was not merely a function of supplier concentration. It was a function of the embeddedness of energy flows within fixed infrastructural and contractual configurations that created high exit costs for all parties.

In parallel, the EU pursued market integration through successive energy policy reforms, culminating in the Third Energy Package of 2009—introducing unbundling rules, third-party access, and regulatory harmonisation aimed at creating a liberalised internal energy market based on competition and transparency (Goldthau and Sitter, 2015). Energy security was increasingly conceptualised in terms of market functioning rather than geopolitical risk. In retrospect, this framing systematically neglected the structural vulnerabilities embedded within both physical and governance domains of the energy network. The gas disputes between Russia and Ukraine in 2006 and 2009 temporarily disrupted supplies to several European countries, exposing transit-dependent infrastructure vulnerability. The annexation of Crimea in 2014 raised further concerns, although major infrastructure projects—including Nord Stream 2—were not fundamentally reconsidered. The persistence of the liberal interdependence paradigm left latent vulnerabilities within the three-domain system largely intact.

An additional layer of complexity emerged from digitalisation. By the late 2010s, electricity and gas networks were increasingly managed through digital platforms capable

Table 1. Comparing the pre-2022 configuration of vulnerability with its post-2022 reconfiguration across the three domains and the emerging critical minerals dimension.
Notes: FSRU: floating storage and regasification units; SCADA: supervisory control and data acquisition; REE: rare earth element; TFEU: Functioning of the European Union; NIS2: Network and Information Systems directive (EU).
Source: Compiled by the author from ENISA (2023); European Commission (2023); IEA (2022, 2023); Sgaravatti *et al.* (2023a).

Domain	Pre-2022 configuration	Post-2022 reconfiguration
Physical infrastructure	Russian pipeline gas ≈40% of EU gas imports (≈155 bcm in 2021); pipeline capacity > 150 bcm/year via Brotherhood pipeline (≈140 bcm), Yamal-Europe pipeline (≈33 bcm), and Nord Stream system (55 bcm + 55 bcm planned); 20–30-year take-or-pay contracts embedding structural rigidity.	Russian pipeline exports ≈27 bcm in 2023 (82%); LNG imports up from ≈80 bcm (2021) to >130 bcm (2023); US ≈47% of EU LNG supply; FSRUs commissioned at Wilhelmshaven, Brunsbüttel, and Lubmin; new chokepoints at US export terminals, FSRU berths, and Hormuz–Panama transit routes.
Digital systems	SCADA and industrial control market dominated by four vendors (Siemens, ABB, Schneider Electric, and Honeywell); vendor concentration attracting little systematic regulatory attention.	Energy sector is among the most targeted sector in Europe; Deutsche Windtechnik intrusion (2022), Ivanti-related incidents in Norway (2023), Sandworm campaigns against Ukrainian grids (2022–2023); regulatory response via Regulation 2024/1366, and CER Directive 2022/2557, unevenly implemented.
Governance	Energy security framed as market functioning (European Parliament and Council of the European Union, 2009a, 2009b); national control of energy mixes under Article 194(2) TFEU; latent fiscal and regulatory asymmetries.	≈€651 bn allocated and earmarked in national fiscal shields (September 2021–mid-2023); Germany >€200 bn "economic defence shield" (€264 bn total); allocations from >7% of GDP (Germany) to <1% in some member states; landlocked states more exposed to transit disruption; NIS2 *directive* transposition uneven at the October 2024 deadline.
Critical minerals (emerging)	Latent dependence embedded in clean-technology supply chains; limited policy salience.	EU imports >98% of REEs, 93% of magnesium, 97% of borates; China: ≈85% of global REE processing and ≈97% of EU solar panel imports; policy response via the Critical Raw Materials Act and Net-Zero Industry Act.

of balancing supply and demand across borders in real time, using SCADA systems and automated algorithms operating across multiple national jurisdictions. Many of these systems relied on technology supplied by a limited number of vendors—Siemens, ABB, Schneider Electric, and Honeywell collectively dominate the European SCADA and industrial control system market—creating a digital chokepoint that attracted little systematic regulatory attention before 2022. The vendor concentration meant that vulnerability in a single widely deployed platform could simultaneously affect transmission system operators across multiple member states, a cross-domain interaction effect that pre-2022 governance frameworks were not designed to address.

Physical infrastructure domain

The war triggered rapid diversification in the physical domain. The EU reduced Russian pipeline gas dependence through three parallel pathways: accelerated LNG import

expansion; emergency deployment of FSRUs; and enhanced utilisation of the existing interconnectors to redirect non-Russian gas supplies. LNG imports increased from approximately 80 bcm in 2021 to more than 130 bcm in 2023, with the United States becoming the single largest supplier, accounting for roughly 47% of EU's LNG imports by 2023 (IEA, 2023). Germany commissioned three FSRUs within 12 months of the invasion—at Wilhelmshaven, Brunsbüttel, and Lubmin—with additional units deployed in Italy and the Netherlands.

The speed of this response was striking. However, the diversification pattern simultaneously created new chokepoints. LNG supply concentration around the US export terminals—Sabine Pass, Freeport, Cove Point—reproduced the supplier-concentration risk that diversification was meant to eliminate, now in a different geopolitical context. FSRU deployment introduced a different form of physical chokepoint: floating infrastructure concentrated in a small number of berths, exposed to weather disruption, and requiring specialist vessels with limited global availability. The Strait of Hormuz and the Panama Canal emerged as critical transit chokepoints for global LNG—maritime bottlenecks whose systemic significance for energy flows has long been recognised (Emmerson and Stevens, 2012). The geographic fixity and capital intensity of LNG infrastructure mean that these new dependencies are embedded for decades. Diversification replaced a Russian pipeline chokepoint with a distributed set of LNG chokepoints; it did not eliminate chokepoint risk.

Digital systems domain

The digital domain received less attention in post-2022 policy than physical supply, but represents a structurally significant vulnerability. European energy systems are increasingly managed through SCADA systems, algorithmic trading platforms, and smart grid technologies. These systems introduce a panopticon dimension to European energy interdependence: dominant positions in digital infrastructure enable surveillance, information asymmetries, and, in adversarial conditions, operational interference.

The ENISA (2023) documents a sustained increase in cyber incidents targeting energy infrastructure, with supply chain attacks and ransomware against energy operators becoming more frequent and sophisticated. Several European SCADA deployments involve software from vendors with potential exposure to third-country jurisdiction—a digital equivalent of the pipeline dependency that physical diversification sought to address. The energy sector was among the most targeted sectors in Europe during 2022, with state-affiliated actors conducting an increasing proportion of attacks.

The empirical record provides specific illustrations that ground theoretical framework in observable events. In April 2022, the German wind energy company Deutsche Windtechnik suffered a cyberattack that disabled remote monitoring of approximately 2,000 wind turbines for several days—a disruption that, while not catastrophic, demonstrated how digital dependencies in renewable energy systems create operational vulnerabilities absent in conventional generation. In January 2023, a coordinated attack on multiple Norwegian energy sector entities exploited vulnerabilities in Ivanti's mobile device management platform, affecting administrative systems at several oil and gas companies. The Sandworm group, attributed to Russian military intelligence, conducted persistent campaigns against Ukrainian energy infrastructure throughout 2022–2023, with techniques and tools that the ENISA (2023) assessed as transferable to Western European grid architectures. These incidents illustrate a pattern in which digital domain serves not only as an independent vector of vulnerability but also as a force multiplier for physical

domain disruptions—the cross-domain interaction effect that the three-domain model identifies as analytically central.

Beyond direct operational disruption, these incidents reveal a more diffused vulnerability: theft or manipulation of operational data from grid management systems could enable adversaries to anticipate grid instabilities, time physical disruptions for maximum impact, or manipulate automated balancing mechanisms. The panopticon effect in the digital domain is therefore not passive surveillance—it is an active precondition for more targeted chokepoint exploitation. The EU's Network Code for Cybersecurity (Regulation 2024/1366) and the Critical Entities Resilience (CER) Directive (2022/2557) represent regulatory response, but implementation remains uneven across member states.

Governance domain

The EU energy governance operates through a complex multi-level system in which authority is distributed among European institutions, national governments, and private actors. Although the EU has developed a relatively integrated internal energy market, member states retain significant control over their national energy mixes, infrastructure planning, and strategic priorities under Article 194(2) TFEU (Goldthau and Sitter, 2015). This configuration allows flexibility but generates coordination challenges when systemic risks affect interconnected infrastructures across multiple jurisdictions.

The crisis revealed these asymmetries with particular clarity. Between September 2021 and mid-2023, European governments allocated and earmarked approximately €651 bn in national fiscal measures to shield households and firms from energy price shocks—but the scale and design varied enormously. Germany alone accounted for above €200 bn through its "economic defence shield," with total German allocations reaching €264 bn; relative allocations across EU ranged from more than 7% of GDP in Germany to less than 1% in some member states (Sgaravatti *et al.*, 2023a). This divergence reflected differences in fiscal capacity rather than energy price exposure, deepening internal market asymmetries at the worst possible moment.

Geography compounded the problem. Coastal states with maritime infrastructure access were better positioned to expand LNG imports and host FSRU terminals. Landlocked countries—Austria, Hungary, Slovakia, and the Czech Republic—remained more dependent on pipeline networks and therefore more exposed to disruption of Russian transit routes. Variations in grid interconnection capacity further shaped national vulnerability: member states with stronger cross-border connections to diverse supply sources proved more resilient, illustrating how the governance domain interacts with the physical infrastructure domain to produce uneven resilience across the integrated system.

Cybersecurity governance presents a particularly acute asymmetry. While both ENISA and Network and Information Systems 2 (NIS2) directive establish common minimum standards for critical infrastructure protection, implementation capacity, enforcement resources, and technical expertise vary enormously. The NIS2 directive transposition deadline of October 2024 found several member states significantly behind schedule, with national cybersecurity agencies in smaller states reporting staffing levels insufficient for the compliance monitoring required by the directive. These gaps represent potential digital chokepoints at the level of regulatory architecture—weaknesses in the governance domain that can be exploited to access the digital domain, which in turn can disrupt the physical domain. Governance asymmetry should therefore be understood as an intrinsic

feature of interconnected energy systems, rather than a temporary policy failure awaiting correction.

Reconfiguration: Critical minerals and emerging dependencies

Whereas Sections 4.1–4.4 examined vulnerabilities that have already materialised, this section turns to a dimension of reconfiguration whose full effects are positioned ahead. The most analytically significant long-term dimension of reconfigured vulnerability concerns critical raw materials. Renewable energy technologies and the electrification of transport and heating depend on minerals, including lithium, cobalt, neodymium, and polysilicon (Vidal *et al.*, 2013). The EU is structurally dependent on non-European sources for the majority of these materials: China processes approximately 85% of global rare earth elements (REEs), supplies approximately 97% of the EU's solar panel imports, and dominates the global battery supply chain (IEA, 2022). The Democratic Republic of Congo dominates global cobalt production.

From the perspective of three-domain model, this creates a new configuration of weaponised interdependence operating in physical and governance domains simultaneously. China's control over critical mineral processing constitutes a chokepoint in global supply chains underpinning European energy transition infrastructure—a structural position analogous to Russia's former control over pipeline gas routes, but operating at the level of materials and manufacturing rather than physical fuel flows. The panopticon effect is also present: dominant processing positions provide access to information about technology deployment rates, component quality standards, and infrastructure plans across importing regions. The geopolitics-of-renewables literature counsels caution here: Overland (2019) argues that mineral dependencies differ from fuel dependencies because minerals can be stockpiled, recycled, and substituted over time. The three-domain model accommodates this caution. Critical minerals constitute latent structural potential rather than active leverage—precisely the category of vulnerability that political conditions may or may not activate.

The scale of dependency warrants empirical specification. The EU imports over 98% of its rare earth elements, 93% of its magnesium, and 97% of its borates from non-European sources, with China as the dominant supplier in most categories (European Commission, 2023). For lithium—essential for battery storage systems that underpin grid flexibility in renewable-heavy electricity systems—the EU depends almost entirely on imports, with processing capacity concentrated in China. The IEA (2022) projects that demand for lithium will increase by a factor of 40 by 2040 under a net-zero scenario, while cobalt demand will increase by a factor of 20. These projections imply that the critical minerals chokepoint will intensify as the energy transition accelerates, creating a temporal dynamic in which diversification away from fossil fuels simultaneously deepens exposure to mineral supply chain vulnerabilities.

This dimension is not reduced by the EU's diversification away from Russian fossil fuels. Accelerated renewable deployment intensifies it. The EU's Critical Raw Materials Act (COM(2023) 160 final; European Commission, 2023) and the Net-Zero Industry Act acknowledge this vulnerability, but the regulatory and investment measures required to substantially reduce critical mineral dependence involve timescales of a decade or more. The weaponised interdependence framework predicts, with uncomfortable clarity, that any actor controlling critical mineral supply chains will possess significant leverage over

European energy security—a structural continuity with pre-2022 Russian gas dependency that supply-centric analyses have not integrated completely.

Discussion

Three findings emerge from the analysis. First, the pre-2022 European energy architecture contained latent vulnerabilities rooted in infrastructural concentration, long-term contractual rigidity, and governance fragmentation that were systematically underestimated under the liberal interdependence paradigm. These features supported efficiency under normal conditions. However, they also created structural asymmetries—critical chokepoints and digital dependencies—that became strategically significant once political conditions activated them in 2022.

Second, diversification reduced dependence on Russian energy but did not eliminate systemic vulnerability; it reconfigured it. New chokepoints emerged in LNG supply chains, FSRU deployment, digital vendor relationships, and critical minerals (Table 1). The concept of structural weaponisation potential—introduced here to describe vulnerability as an emergent property of networked systems, independent of any actor's intention—captures this condition more precisely than the binary of dependence versus diversification. European energy systems are structurally weaponisable regardless of whether any state actor chooses to exploit that vulnerability at any given moment.

Third, governance asymmetry among member states functions as an endogenous amplifier of systemic vulnerability. Uniform EU obligations cannot produce uniform outcomes when applied to structurally diverse national systems. The distributional consequences of the crisis response—falling disproportionately on member states with limited fiscal capacity and constrained infrastructure endowment—raise legitimacy concerns that are politically significant, independent of their economic magnitude. Where adjustment costs concentrate in fiscally constrained or infrastructurally disadvantaged member states, they translate into political pressure against the collective EU energy governance, creating a feedback loop between distributional inequality and collective action capacity.

The principal theoretical contribution is the extension of weaponised interdependence from financial and digital networks to physical energy infrastructure through the three-domain model. This extension reveals that the chokepoint and panopticon effects operate differently in infrastructure-heavy sectors than in the domains where the concept was originally developed. Physical infrastructure introduces geographic fixity, path dependencies, and capacity constraints that produce cross-domain interaction effects not captured by the original framework. The three-domain model operationalises the concept for application to any sector characterised by networked physical infrastructure, digital management systems, and multi-level governance—a contribution relevant beyond the European energy case.

Conclusions

The Russia–Ukraine war fundamentally transformed the structure of European energy security by exposing and activating vulnerabilities that had been embedded within interconnected energy systems for decades. European policymakers had interpreted energy relations with Russia through the lens of economic interdependence, assuming that dense trade relationships and shared infrastructure would promote stability and mutual restraint. The events of 2022 demonstrated the limitations of that assumption and revealed how

interdependence—when embedded within specific network configurations—becomes a source of systemic vulnerability under conditions of geopolitical conflict.

The analysis returns three findings, developed in Section 5: latent structural vulnerability that market liberalisation systematically obscured; the reconfiguration, rather than elimination, of vulnerability through post-2022 diversification; and governance asymmetry as an endogenous amplifier of systemic risk. Russia's weaponisation of gas supply did not create these vulnerabilities; it activated them, converting latent structural potential into operationalised coercive leverage. Conceptually, the notion of structural weaponisation potential names the condition that these findings describe—networked systems generate vulnerability as an emergent property of their architecture, independent of any actor's intention to exploit it—a condition that the pre-2022 European energy system exemplified and that the post-2022 system has reproduced in a new form.

Several limitations should be acknowledged. The study relies on publicly available documents, and no primary fieldwork was conducted. The focus on the EU as a collective actor simplifies considerable variation among individual member states. Quantitative network analysis of energy infrastructure topologies would provide valuable empirical grounding. Future research should trace how the shift towards renewables reconfigures the distribution of critical nodes—particularly as critical mineral dependencies intensify—and develop empirical analysis of the digital domain vulnerabilities identified here.

The European experience following the Russia–Ukraine war constitutes a critical case study of how deeply embedded interdependence can transform from a source of stability into a vector of systemic risk. As the global energy system undergoes structural transformation driven by decarbonisation, digitalisation, and geopolitical realignment, the analytical framework developed here provides a basis for examining how emerging energy networks reshape patterns of vulnerability and resilience. Managing interdependence—rather than attempting to eliminate it—remains the central challenge for energy security governance in the decades ahead. The question is whether governance can evolve at the speed the transformation demands.

Funding

This research received no external funding.

Data Availability Statement

Data sharing not applicable. No new data was created or analysed in this study.

Disclosure Statement

No potential conflict of interest was reported by the author. The author read and agreed to the published version of the manuscript.

AI Use Declaration

In preparing this manuscript and its revision, the author used Claude (Anthropic; claude-sonnet-4-6 and claude-fable-5) to assist with prose revision at the sentence level, citation formatting, and reference verification against primary sources. All arguments, evidence, source selections, and analytical claims are that of author's. The author reviewed and edited all AI-assisted output and takes full responsibility for the content of the manuscript.

References

Baldwin, D.A. (1980) 'Interdependence and power: A conceptual analysis', *International Organization*, 34(4), pp. 471–506. doi: 10.1017/S0020818300018828.

Balmaceda, M.M. (2021) *Russian energy chains: The remaking of technopolitics from Siberia to Ukraine to the European Union*. New York, NY: Columbia University Press.

Bowen, G.A. (2009) 'Document analysis as a qualitative research method', *Qualitative Research Journal*, 9(2), pp. 27–40. doi: 10.3316/QRJ0902027.

Drezner, D.W. (2021) 'Introduction: The uses and abuses of weaponized interdependence', in Drezner, D.W., Farrell, H. and Newman, A.L. (eds.) *The uses and abuses of weaponized interdependence*. Washington, DC: Brookings Institution Press, pp. 1–18.

Emmerson, C. and Stevens, P. (2012) *Maritime choke points and the global energy system: Charting a way forward.* Briefing paper EERG BP 2012/01. London: Chatham House, Royal Institute of International Affairs.

European Commission (2014) *European energy security strategy* (COM(2014) 330 final). Brussels: European Commission.

European Commission (2022) *REPowerEU plan* (COM(2022) 230 final). Brussels: European Commission.

European Commission (2023) *EU's critical raw materials act* (COM(2023) 160 final). Brussels: European Commission.

European Parliament and Council of the European Union (2009a) *Directive 2009/72/EC of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC*, Official Journal of the European Union, L 211, 14 August 2009, pp. 55–93.

European Parliament and Council of the European Union (2009b) *Directive 2009/73/EC of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC*, Official Journal of the European Union, L 211, 14 August 2009, pp. 94–136.

European Union Agency for Cybersecurity (ENISA) (2023) *ENISA threat landscape 2023*. Attiki: ENISA.

Farrell, H. and Newman, A.L. (2019) 'Weaponized interdependence: How global economic networks shape state coercion', *International Security,* 44(1), pp. 42–79. doi: 10.1162/isec_a_00351.

Farrell, H. and Newman, A.L. (2023) *Underground empire: How America weaponized the world economy*. New York, NY: Henry Holt.

Goldthau, A. and Sitter, N. (2015) *A liberal actor in a realist world: The European Union regulatory state and the global political economy of energy*. Oxford: Oxford University Press. doi: 10.1093/acprof:oso/9780198719595.001.0001.

Goldthau, A. and Sitter, N. (2022) 'Whither the liberal European Union energy model? The public policy consequences of Russia's weaponization of energy', *EconPol Forum,* 23(6), pp. 4–7. RePEc:ces:epofor:v:23:y:2022:i:06:p:4-7.

International Energy Agency (IEA) (2022) *World energy outlook 2022*. Paris: IEA.

International Energy Agency (IEA) (2023) *Gas market report Q2-2023*. Paris: IEA.

Keohane, R.O. and Nye, J.S. (1977) *Power and interdependence: World politics in transition*. Boston, MA: Little Brown.

Kuzemko, C., Blondeel, M., Dupont, C. and Brisbois, M.C. (2022) 'Russia's war on Ukraine, European energy policy responses and implications for sustainable transformations', *Energy Research and Social Science*, 93, p. 102842. doi: 10.1016/j.erss.2022.102842.

Overland, I. (2019) 'The geopolitics of renewable energy: Debunking four emerging myths', *Energy Research and Social Science*, 49, pp. 36–40. doi: 10.1016/j.erss.2018.10.018.

Sgaravatti, G., Tagliapietra, S., Trasi, C. and Zachmann, G. (2023a) *National policies to shield consumers from rising energy prices*. Dataset version of 26 June 2023. Brussels: Bruegel. doi: 10.64153/LQHK8283.

Sgaravatti, G., Tagliapietra, S. and Zachmann, G. (2023b) *Adjusting to the energy shock: The right policies for European industry* (policy brief 11/2023). Brussels: Bruegel.

Siddi, M. (2023) *European energy politics: The green transition and EU–Russia energy relations*. Cheltenham: Edward Elgar.

Vidal, O., Goffé, B. and Arndt, N. (2013) 'Metals for a low-carbon society', *Nature Geoscience*, 6(11), pp. 894–896. doi: 10.1038/ngeo1993.

Wright, S. (2017) 'Qatar's LNG: Impact of the changing East-Asian market', *Middle East Policy*, 24(1), pp. 154–165. doi: 10.1111/mepo.12257.

Yergin, D. (2006) 'Ensuring energy security', *Foreign Affairs*, 85(2), pp. 69–82. doi: 10.2307/20031912.

Zha, D. (2006) 'China's energy security: Domestic and international issues', *Survival*, 48(1), pp. 179–190. doi: 10.1080/00396330600594322.