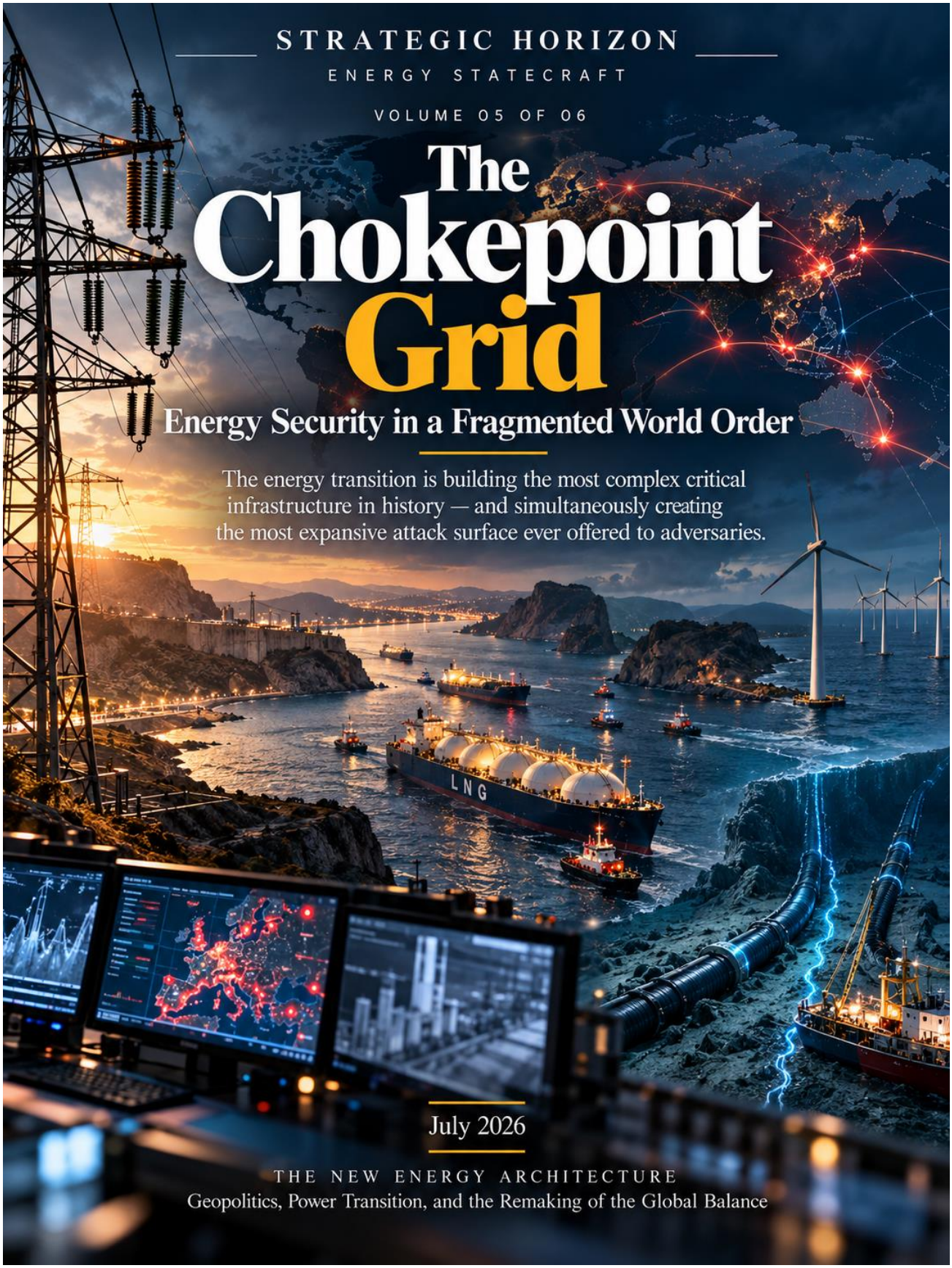

STRATEGIC HORIZON
ENERGY STATECRAFT
VOLUME 05 OF 06
The Chokepoint Grid
Energy Security in a Fragmented World Order
The energy transition is building the most complex critical infrastructure in history — and simultaneously creating the most expansive attack surface ever offered to adversaries.
LNG
July 2026
THE NEW ENERGY ARCHITECTURE
Geopolitics, Power Transition, and the Remaking of the Global Balance

THE NEW ENERGY ARCHITECTURE

Geopolitics, Power Transition, and the Remaking of the Global Balance

Vol. 5 of 6

The Chokepoint Grid

Energy Security in a Fragmented World Order

The energy transition is building the most complex critical infrastructure in history — and simultaneously creating the most expansive attack surface ever offered to adversaries

July 2026

THE NEW ENERGY ARCHITECTURE — 6-Volume Series

Vol. 1–4 (published): Petro-States | Electro-Hegemon | Hydrogen Chessboard | Nuclear Renaissance

Vol. 5 (this volume): The Chokepoint Grid — Energy Security in a Fragmented World Order

Vol. 6: Energy Poverty and the Global South Revolt — The Fractured Transition (forthcoming)

Executive Summary

The energy transition is not merely a technological reordering of supply chains. It is the construction of an entirely new physical and digital infrastructure layer — one that is more geographically distributed, more digitally interconnected, and more dependent on vulnerable chokepoints than the fossil fuel system it is replacing. In a world of accelerating great-power competition, every new infrastructure node is also a new target.

The evidence from 2024-2026 is unambiguous. Cyberattacks on US energy utilities increased by 70% in 2024, reaching 1,162 incidents. Sixty-seven percent of energy organisations faced ransomware attacks, with 80% resulting in data encryption. The average recovery cost reached $3.12 million per incident. State-sponsored actors — Russia's Sandworm, China's Volt Typhoon, Iran's Cyber Av3ngers — have pre-positioned malware in Western energy infrastructure awaiting activation. The 2022 Nord Stream sabotage demonstrated that undersea energy infrastructure in contested waters is physically vulnerable to state-sponsored destruction without attribution. The 2026 Iran war produced direct strikes on South Pars gas facilities and Strait of Hormuz disruption simultaneously.

This volume maps the chokepoint grid across five vulnerability vectors: the maritime bottlenecks through which fossil fuels flow; the undersea cable networks through which renewable electricity and communications travel; the LNG terminals anchoring Europe's post-Russian energy architecture; the smart grid systems whose digital interconnection creates systemic cyber exposure; and the new manufacturing chokepoints of the energy transition — transformer bottlenecks, electrolyser supply chains, HALEU fuel networks, and Chinese clean tech lock-in. The conclusion is discomforting: the green transition is not reducing Western energy chokepoint exposure. In several important respects, it is increasing it.

Keywords: *chokepoint, hybrid warfare, energy infrastructure, Nord Stream, Strait of Hormuz, undersea cable, LNG terminal, smart grid, SCADA, Volt Typhoon, Sandworm, Baltic Sentry, Bab el-Mandeb, Strait of Malacca, load-altering attack, critical infrastructure, transformer bottleneck*

SECTION 1 The Chokepoint Concept: Old Geography, New Architecture

Energy security has always been a geography problem. The global energy system — fossil fuels concentrated in a small number of producing regions, transported through a limited number of maritime and pipeline corridors to consuming markets — creates chokepoints whose control or disruption determines energy price and availability for billions of people. What the energy transition is doing is not eliminating chokepoints. It is multiplying them, digitising them, and distributing them into new and often less well-defended locations.

The classic chokepoints remain operative. The Strait of Hormuz — 34 kilometres wide at its narrowest — handles approximately 20% of global seaborne oil and 20% of global LNG. The Strait of Malacca — through which approximately 80,000 vessels pass annually — is the primary corridor for crude oil and LNG supplying China, Japan, South Korea, and Taiwan. The Bab el-Mandeb connects the Red Sea to the Gulf of Aden and handles approximately 10% of global trade. The Houthi missile and drone campaign in the Red Sea throughout 2024-2026, which forced more than 100 container vessels to reroute around the Cape of Good Hope, demonstrated the real-world cost of a chokepoint threat even when not fully closed: shipping costs tripled, transit times increased by 10-14 days, and energy cost premiums contributed measurably to European inflation.

The energy transition adds three new chokepoint categories. First, electrical transmission infrastructure: undersea HVDC cables connecting offshore wind farms, cross-border electricity interconnectors, and submarine cables carrying both power and communications. Second, digital control systems: smart grids, SCADA systems, and industrial control systems managing the increasingly complex interplay of variable renewables, storage, and transmission — interconnected, remotely operated, and running on commercial software with known vulnerabilities. Third, manufacturing chokepoints: transformer production concentrated in a handful of facilities, electrolyser manufacturing dominated by Chinese suppliers, and semiconductor-dependent grid management systems. The energy transition's supply chain dependencies documented in Volumes 2, 3, and 4 of this series are themselves structural chokepoints of a new kind.

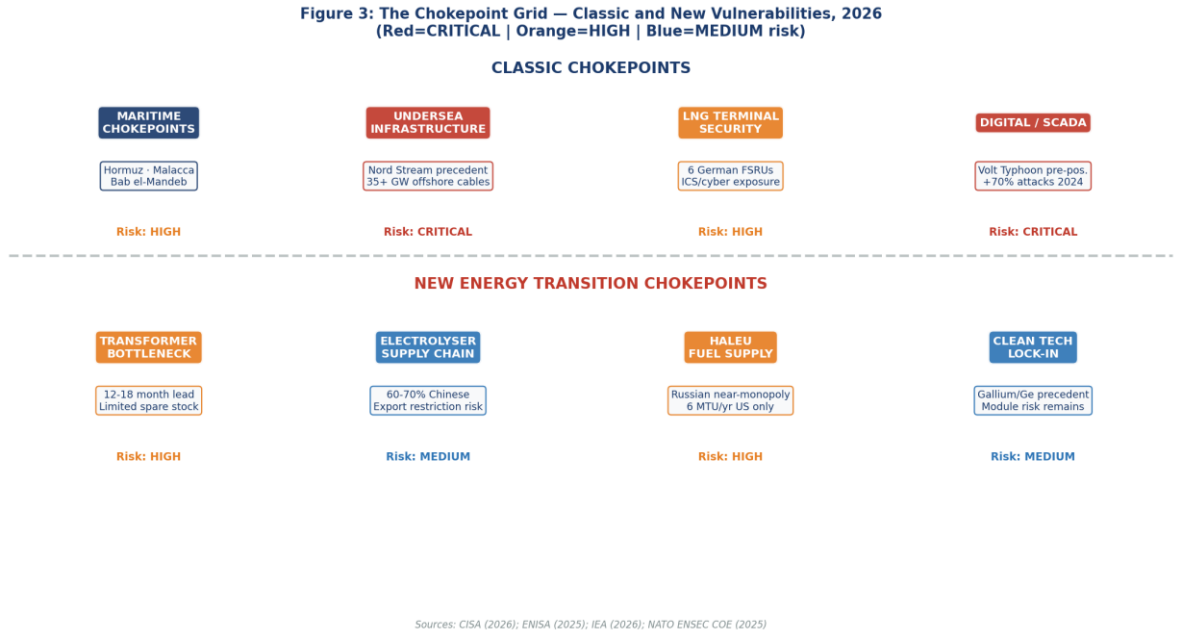


Figure 3: The Chokepoint Grid — Classic and New Vulnerabilities, 2026. Classic maritime chokepoints have been joined by new transition-era chokepoints: transformers, electrolysers, HALEU fuel, and Chinese clean tech lock-in. Sources: CISA (2026); ENISA (2025); IEA (2026).

SECTION 2 The Physical Attack Surface: Underwater and Underground

The Baltic Precedent and Subsea Assets

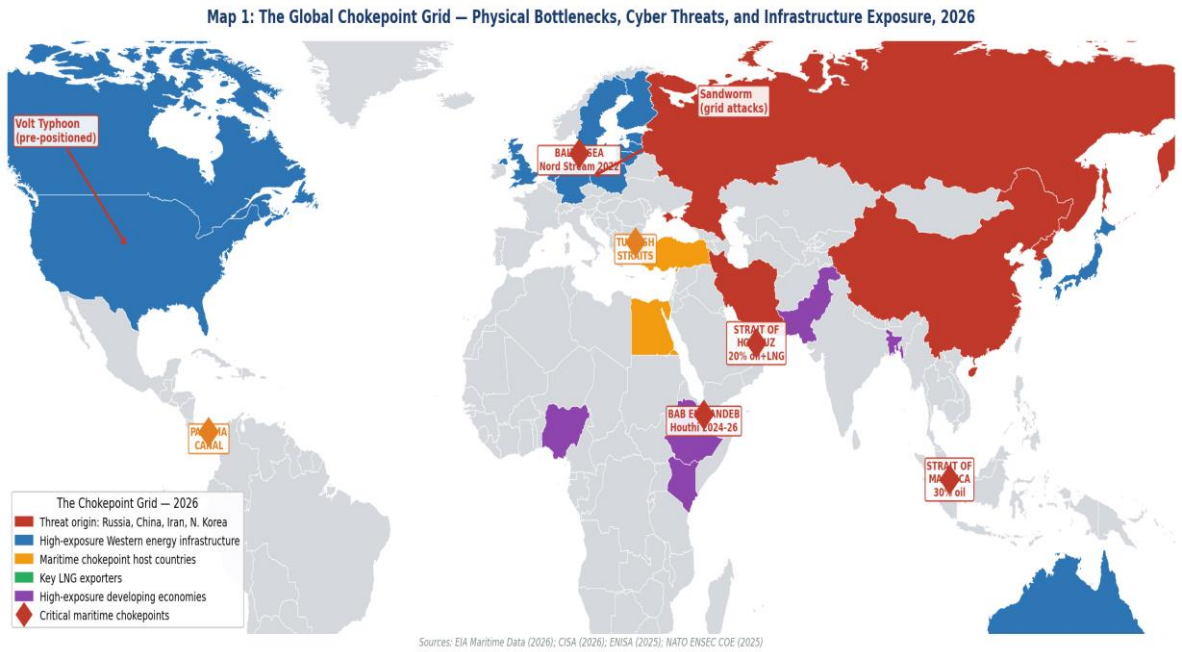
The September 2022 Nord Stream pipeline sabotage was a watershed event in energy infrastructure vulnerability. Four simultaneous explosions on the Baltic Sea floor ruptured three of the four strings of Nord Stream 1 and 2, releasing approximately 778 million cubic metres of methane and permanently destroying

infrastructure worth approximately $10 billion. The political investigation has been protracted and contested. The operational lesson is unambiguous: submarine critical energy infrastructure in contested maritime regions can be destroyed by a state actor willing to accept consequences, with limited immediate attribution and even more limited accountability.

The Nord Stream precedent has accelerated recognition that the Baltic and North Sea — increasingly home to the offshore wind infrastructure on which Europe's energy transition depends — are physically contested spaces. By 2026, the European offshore wind installed base in the Baltic and North Sea exceeds 35 GW, connected to onshore grids through hundreds of kilometres of submarine export cables. Each cable is a vulnerable chokepoint: repair vessels require specialised equipment available from a small number of global operators, cable repair operations take weeks in good weather and are impossible in severe Baltic winter conditions, and damaged cables in deep water can take months to restore. NATO's Baltic Sentry initiative — launched in January 2025 — has elevated undersea infrastructure protection to a collective defence doctrine question: enhanced naval surveillance, seabed monitoring, and rapid repair capacity were established specifically in response to demonstrated Russian grey-zone pressure against Baltic infrastructure.

The October 2023 Baltic Connector incident confirmed that non-explosive physical interference achieves significant disruption at low cost and low risk to the attacker: a vessel suspected of anchor-dragging severed the Finland-Estonia gas pipeline and a communications cable simultaneously. NATO's assessment is that Russian strategy has incorporated deliberate testing of infrastructure vulnerability as a deniable grey-zone pressure instrument — neither an act of war nor a purely commercial incident, but a form of structured ambiguity designed to avoid triggering Article 5 while imposing real costs.

Undersea communications cables present an identical vulnerability profile. Approximately 95% of international internet and financial data transits undersea fibre optic cables, of which approximately 600 active systems exist globally. SCADA systems, energy trading platforms, and grid management interfaces all depend on this internet connectivity. The concentration of cable landing stations in a small number of coastal locations creates additional chokepoint risk, as a small number of physical interventions could affect disproportionate shares of global data traffic.



Map 1: The Global Chokepoint Grid — Physical Bottlenecks, Cyber Threat Origins, and Infrastructure Exposure, 2026. Sources: EIA Maritime Data (2026); CISA (2026); ENISA (2025); NATO ENSEC COE (2025).

Nord Stream Precedent — The Operational Lesson

Date: September 26, 2022 | Location: Baltic Sea, 70–80m depth | Method: Four simultaneous underwater explosions

Infrastructure destroyed: Three of four pipeline strings permanently inoperable | Value: ~$10 billion

Methane released: ~778 million cubic metres | Attribution: contested; zero accountability

Operational lesson: Submarine critical energy infrastructure can be destroyed with limited attribution and no immediate accountability

NATO response: Baltic Sentry (Jan 2025) elevated undersea infrastructure protection to collective defence doctrine

Consequence for transition: 35+ GW of offshore wind cables in Baltic/North Sea face identical physical vulnerability

SECTION 3 LNG Terminals: The New Strategic Nodes

Europe's post-Russian energy architecture is anchored in LNG terminal infrastructure built at speed and scale between 2022 and 2025. Six floating storage and regasification units (FSRUs) were constructed in Germany alone in approximately 18 months — the fastest energy infrastructure construction programme in European history. The Netherlands, France, Italy, Belgium, Poland, Finland, and Greece have all expanded LNG import capacity. European LNG import capacity has approximately doubled since 2021.

The Multi-Dimensional Threat Profile

FSRUs are high-value, highly concentrated strategic assets — moored permanently at coastal berths, operating at the intersection of maritime port security and high-pressure gas distribution. This creates a threat profile that combines elements of port security, maritime security, and critical infrastructure protection in ways that existing regulatory frameworks were not designed to address. The 2026 Iran war crystallised the full supply chain dimension of this vulnerability: Iranian strikes on South Pars processing facilities and QatarEnergy's subsequent force majeure on LNG export contracts forced European utilities into severe spot-market bidding wars, demonstrating that LNG terminal vulnerability encompasses the entire chain from wellhead to regasification — not merely the European import terminals.

The cyber dimension of LNG terminal vulnerability deserves particular attention. Industrial control systems at LNG facilities — managing cryogenic liquefaction processes, pressurised regasification systems, and safety interlocks preventing catastrophic overpressure events — are increasingly networked and remotely accessible. The 2021 Florida water treatment facility intrusion demonstrated that ICS systems can be accessed and manipulated through remote access tools. An adversary with access to an LNG terminal's ICS could, in principle, disrupt operations or interfere with safety systems without physical access to the site. The US Energy Department documented a 70% increase in cyberattacks on energy utilities in 2024 (from 689 to 1,162 incidents). Sixty-seven percent of energy organisations faced ransomware attacks, with 80% resulting in data encryption, at $3.12 million average recovery cost per incident.

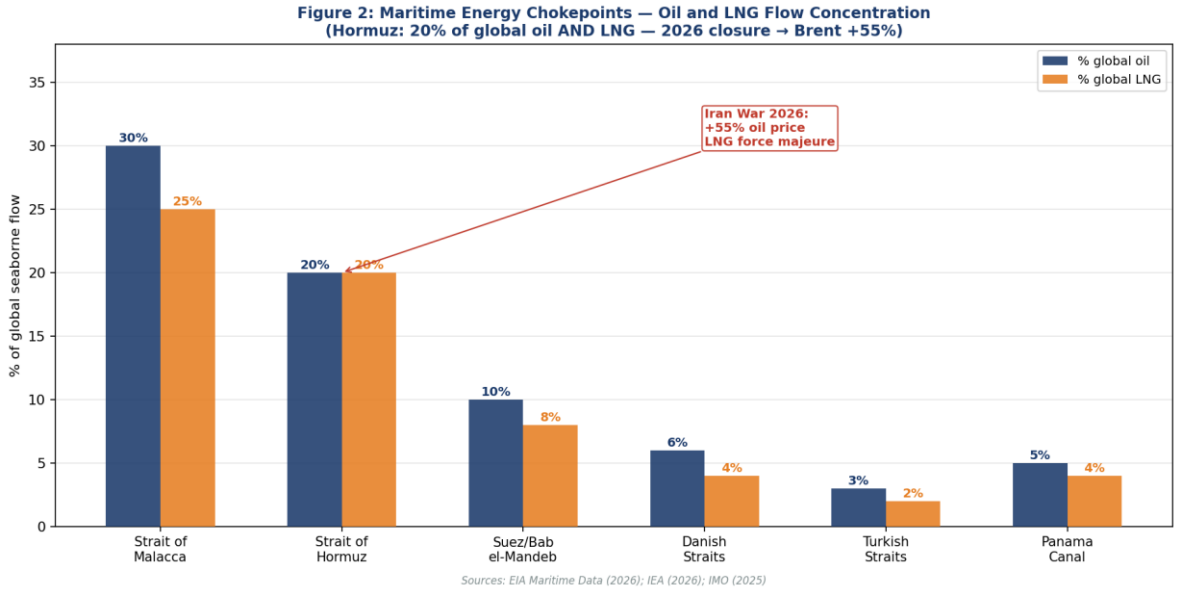


Figure 2: Maritime Energy Chokepoints — Oil and LNG Flow Concentration. Hormuz carries 20% of global oil AND 20% of LNG simultaneously. Iran War 2026: Hormuz disruption produced +55% oil price and LNG force majeure cascade. Sources: EIA Maritime Data (2026); IEA (2026); IMO (2025).

SECTION 4 Smart Grids, SCADA, and the Digital Attack Surface

The digitalisation of energy infrastructure is the most consequential and least discussed dimension of the chokepoint problem. Managing variable renewable output, integrating distributed generation from millions of rooftop solar systems, coordinating demand response from EV chargers and heat pumps, and optimising cross-border electricity flows all require digital control systems — and digital control systems are attack surfaces.

SCADA systems and industrial control systems that manage electricity grids, gas pipelines, and LNG terminals were originally designed for isolated, proprietary networks without internet connectivity. The digitalisation imperative has connected many of these systems to corporate networks and in some cases to the internet — dramatically expanding their attack surface without commensurate expansion of security architecture. ENISA's 2025 Threat Landscape report documents that Operational Technology attacks now represent 18.2% of all threats against energy infrastructure, up from less than 5% in 2020.

Key Digital Vulnerabilities — 2026 Data

Three threat vectors define the state-sponsored cyber threat to energy infrastructure:

Dormant Malware Pre-Positioning: Joint advisories from CISA and the NSA confirmed that China's Volt Typhoon has embedded dormant malware within US power grid networks. The objective is not espionage but pre-positioned disruption — awaiting activation in the event of a conflict over Taiwan. Russia's Sandworm caused actual grid blackouts in Ukraine in 2015 and 2016, and is assessed as having pre-positioned equivalent capabilities against European energy networks. Iran's Cyber Av3ngers attacked industrial control systems at US water treatment facilities in late 2023, demonstrating ICS capability and willingness to target critical infrastructure.

Load-Altering Edge Attacks: Advanced Metering Infrastructure and connected EV charging networks represent a novel attack vector. Coordinated, malicious manipulation of thousands of high-wattage EV chargers can inject artificial load spikes, triggering frequency instability and cascading grid failures — achieving grid effects previously requiring attacks on generation or transmission assets, but from consumer-edge devices with minimal physical access requirements. The April 2025 Energies journal analysis documented this EV charging attack vector as an emerging strategic threat.

Satellite Signal Dependency: Modern grid protection relays rely on GPS timing signals for microsecond synchronisation. GPS jamming and spoofing — widely documented in Baltic and Eastern Mediterranean maritime zones since 2019 — threatens the automated safety protocols of high-voltage transmission networks and the SCADA systems of remote renewable installations that rely on satellite-dependent communications.

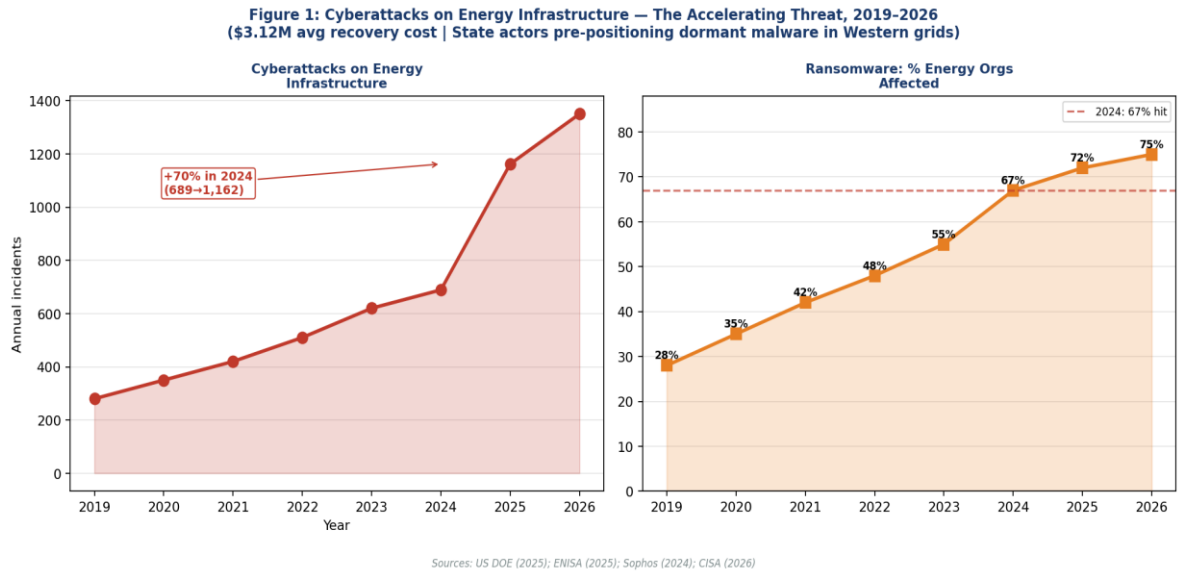


Figure 1: Cyberattacks on Energy Infrastructure — The Accelerating Threat, 2019–2026. +70% in 2024 (689→1,162 incidents); 67% of energy organisations hit by ransomware; $3.12M average recovery cost. Sources: US DOE (2025); ENISA (2025); Sophos (2024); CISA (2026).

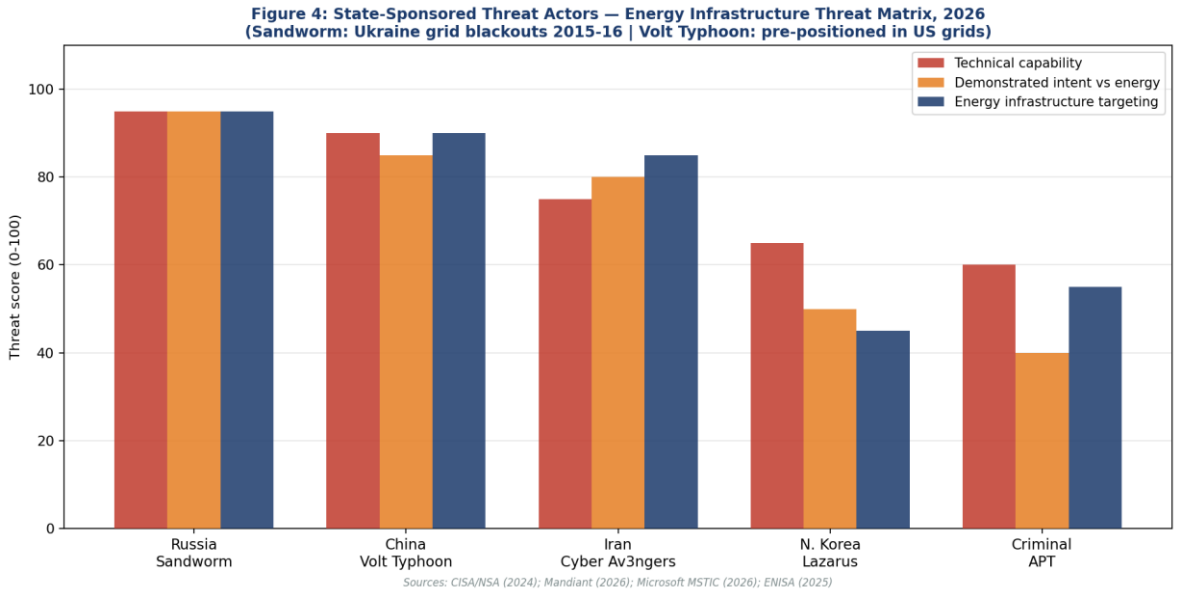


Figure 4: State-Sponsored Threat Actors — Energy Infrastructure Threat Matrix, 2026. Sandworm demonstrated actual grid blackout capability (Ukraine 2015-16). Volt Typhoon pre-positioned in US energy networks. Cyber Av3ngers attacked ICS systems 2023. Sources: CISA/NSA (2024); Mandiant (2026); Microsoft MSTIC (2026).

SECTION 5 The New Chokepoints of the Energy Transition

The energy transition's manufacturing chokepoints fall into four categories, each with distinct strategic risk profiles.

Large Power Transformer Bottleneck: The energy transition's least-discussed structural constraint. Large power transformers (LPTs) take 12-18 months to manufacture, cost $3-10 million per unit, and are produced by a small number of manufacturers globally. The US grid operates approximately 2,500 large transformers, most beyond their design life. A successful physical or cyber attack damaging a small number of strategic transformers could require months-long restoration with no spare equipment available. The US DOE's Strategic Transformer Reserve covers only a fraction of the at-risk inventory.

Electrolyser Supply Chain: Chinese manufacturers control approximately 60-70% of global electrolyser production at a cost structure Western competitors cannot yet match. A government committing to a green hydrogen pathway without a non-Chinese electrolyser supply chain has traded dependence on Russian gas for dependence on Chinese industrial equipment — with similar strategic leverage implications and significantly less political awareness of the exposure.

HALEU Fuel Supply: Russian TENEX's near-monopoly on commercial HALEU production, combined with HALEU requirements of most next-generation reactor designs, creates a fuel supply chokepoint for the advanced nuclear deployment that Western governments are counting on for firm low-carbon baseload. Centrus Energy's Piketon facility at 6 MTU/year is demonstration-scale only.

Chinese Clean Tech Lock-In: China's gallium and germanium export restrictions (2023), graphite controls (2024), and rare earth export permit requirements (2025) are the first instances of clean energy supply chain weaponisation. If China were to apply similar restrictions to solar wafers, battery cells, or electrolyser components, the impact on Western renewable deployment would be severe and not immediately remediable — a structural risk that the Bypass Dividend of domestic supply chain investment has not yet adequately addressed.

The New Transition Chokepoints — Risk Summary

TRANSFORMER BOTTLENECK (HIGH): 12-18 month manufacturing lead; limited spare inventory; US strategic reserve covers fraction of at-risk stock

ELECTROLYSER SUPPLY (MEDIUM-HIGH): 60-70% Chinese manufacture; export restriction risk mirrors gallium/germanium 2023 precedent

HALEU FUEL (HIGH): Russian near-monopoly on commercial production; Centrus Piketon at 6 MTU/yr is demonstration-scale only

CHINESE CLEAN TECH LOCK-IN (CRITICAL): Export restrictions on upstream materials already exercised; module/cell-level restrictions remain available leverage

SATELLITE DEPENDENCY (MEDIUM): GPS timing for grid protection relays; Starlink SCADA in remote renewables; jamming documented Baltic/Black Sea since 2019

SECTION 6 Strategic Policy Imperatives: Hardening the Grid

Three integrated policy pillars define the hardening agenda for the Chokepoint Grid.

Physical Resilience and Subsea Governance

The most urgent physical infrastructure imperative is undersea cable protection. The Baltic Sentry framework provides the model — enhanced naval patrol, seabed monitoring, and rapid repair capacity — that should be extended to the North Sea offshore wind cable networks and major transatlantic and trans-Mediterranean cable clusters. The practical requirements: a standing allied maritime patrol capability specifically tasked with infrastructure protection, pre-positioned cable repair vessels with guaranteed rapid deployment authority, and a classified registry of highest-consequence cable segments whose protection should be treated equivalent to NATO territory defence. A multilateral LNG Supply Chain Security Protocol — establishing rules of engagement for the protection of LNG carriers, export terminals, and import facilities in times of regional conflict — would provide a governance framework currently absent from international maritime law.

Digital Hardening and OT Isolation

LNG terminal security requires mandatory OT/IT separation (air-gapping critical control systems from corporate networks), regular adversarial red-teaming of ICS, supply chain security requirements for all software and hardware integrated into terminal control systems, and incident response plans with pre-designated restoration authorities. The smart grid digitalisation programme requires a fundamental rethink of its security architecture — deploying Hardware Security Modules (HSMs) in all grid-edge assets, enforcing mandatory Software Bills of Materials (SBOM) for connected devices, and executing adversarial red-teaming of utility SCADA platforms backed by government threat intelligence. The EU's NIS2 Directive, in force since October 2024, establishes cybersecurity requirements for critical infrastructure — but energy sector compliance with OT-specific requirements is lagging significantly across member states.

Strategic Reserves and Industrial Policy

The manufacturing chokepoint problem requires industrial policy responses modelled on the CHIPS Act — but have not yet received comparable political attention or funding. A Strategic Energy Infrastructure Reserve covering large power transformers, submarine cable inventory, and key grid protection components should be established as a NATO-allied collective resilience measure. Electrolyser manufacturing capacity requires IRA-style domestic content requirements to prevent the hydrogen economy of the 2030s from replicating the solar panel dependency dynamic. The diplomatic dimension — updating maritime chokepoint governance frameworks to reflect LNG dependency — remains the most underdeveloped element of the chokepoint hardening agenda.

Conclusion: The Sovereign Transition Window

The energy transition's security challenge is not a temporary problem to be solved once new infrastructure is in place. It is a permanent feature of an energy system that is simultaneously more distributed, more digitally interconnected, and more dependent on concentrated manufacturing and material chokepoints than the fossil fuel system it is replacing.

The Nord Stream sabotage, the Houthi Red Sea campaign, the Iran war's LNG disruption, the documented pre-positioning of state-sponsored malware in Western grid systems, and the structural supply chain dependencies of solar, battery, and electrolyser manufacturing all point to the same conclusion: energy infrastructure is now a primary domain of great-power competition, not a protected civilian asset outside the logic of geopolitical contestation.

The energy transition is not building a more resilient energy system in the near term. It is building a more efficient, lower-carbon, and ultimately more sovereign energy system — but one whose transition period creates a specific and exploitable vulnerability window during which adversaries have strong incentives to target new infrastructure before it is adequately hardened, test governance gaps before they are closed, and demonstrate that the dependency shift from Russian gas to Chinese manufacturing is not the liberation its advocates claim.

Hardening that sovereign transition window requires physical, digital, and diplomatic measures delivered simultaneously and at allied scale. Countries that treat chokepoint security as a secondary infrastructure compliance issue — rather than as the primary strategic condition for a successful energy transition — will find the transition window closing not because the technology failed, but because the architecture was left undefended.

Volume 6 of the New Energy Architecture series will examine Energy Poverty and the Global South Revolt — the fracture between countries that can afford to build the secure, diversified, resilient energy transition described in these volumes, and the countries that cannot.

The New Energy Architecture — Series Overview

Vol. 1 (published): The Twilight of Petro-States

Vol. 2 (published): The Electro-Hegemon — China's Clean Tech Monopoly

Vol. 3 (published): The Hydrogen Chessboard

Vol. 4 (published): The Nuclear Renaissance — SMRs, Rosatom, Fusion, Thorium

Vol. 5 (this volume): The Chokepoint Grid — Energy Security in a Fragmented World Order

Vol. 6: Energy Poverty and the Global South Revolt — The Fractured Transition

References and Key Sources

Official and Government Sources

- CISA/NSA (2024). Volt Typhoon Pre-Positioning in US Critical Infrastructure — Joint Advisory.
- US DOE (2025). Cyberattacks on Energy Utilities — Annual Threat Report.
- ENISA (2025). Threat Landscape for the Energy Sector. EU Agency for Cybersecurity.
- NATO ENSEC COE (2025). Energy Security and Hybrid Warfare — Baltic Region Assessment.
- EIA (2026). Maritime Chokepoints — Global Energy Flow Data.
- NIS2 Directive (2024). EU Directive — Energy Sector Implementation.

Research and Intelligence

- Mandiant / Google Cloud (2026). APT Groups Targeting Energy Infrastructure — Annual Report.
- Microsoft MSTIC (2026). Volt Typhoon: China State-Sponsored Actor Targeting Critical Infrastructure.
- Sophos (2024). State of Ransomware in Energy, Oil and Utilities 2024.
- Energies Journal (2025). EV Charging Infrastructure as Load-Altering Cyber Attack Vector. April 2025.
- Chatham House (2026). Offshore Wind Security in the North Sea.
- IISS (2025). Hybrid Warfare and Critical Infrastructure — Maritime Security Chapter.
- Bruegel (2026). LNG Terminal Security in Europe — Policy Brief.

The New Energy Architecture | Vol. 5 of 6 | July 2026 | Prepared for academic and policy research purposes.