

Protecting critical infrastructure from physical and hybrid threats

Alexandr Burilkov
Andrea Pahon
Diana Sarah Ondrejkořová

Protecting critical infrastructure from physical and hybrid threats

Alexandr Burilkov, Andrea Pahon, Diana Sarah Ondrejčovičová

September 2026

GLOBSEC Geotech Center

www.globsecusfoundation.org

www.globsec.org

Disclaimer:

All of the views expressed in this piece are those of the authors and thus do not necessarily represent the official position of GLOBSEC, GLOBSEC US Foundation or associated partners

This paper was produced with financial support from the Ministry for Foreign Affairs of Sweden. GLOBSEC donors do not determine any of this paper's conclusions.

Executive summary

National protection systems capture only part of the cross-border distribution of infrastructure risk. Critical-infrastructure protection remains organised predominantly through national jurisdictions, while ownership, operational dependencies, supply chains, and disruption effects frequently extend across several states. Nationally important assets and regionally important functions therefore do not always coincide. Cross-border assessments should begin with the societal and strategic functions that must continue and trace the assets, alternative routes, operators, spare capacity, and dependencies required to sustain them.

Attribution is complicated by the growing separation between the actor carrying out an attack, the networks or capabilities enabling it, and its wider effects. State-linked sabotage remains the principal foreign-policy concern. Meanwhile, criminals, extremists, and other non-state actors may operate independently while drawing on technologies, information, skills, and networks that cross borders. Transnational activity alone does not establish state direction or a hybrid campaign. Analysis should distinguish actor, motive, linkage and enablement, and effect, while treating foreign provenance, capability diffusion, sponsorship, and state direction as separate evidentiary questions.

Europe already possesses substantial resilience architecture; the remaining weaknesses are primarily operational. EU and NATO arrangements cover risk assessment, cross-border consultation, public-private cooperation, incident coordination, and recovery planning (European Parliament and Council 2022; Council of the European Union 2024; European Commission and High Representative 2025a; NATO 2026). Gaps remain in the exchange of usable threat and asset information, coordination between governments and operators, and access to scarce repair capacity during simultaneous disruptions. Public authorities and operators hold different parts of the information and capabilities required for resilience, making advance coordination necessary.

Sustained hostile pressure raises continuity questions that existing peacetime arrangements address only partially. Ukraine and the 2026 Gulf conflict show how repair, protection, and continuity can become recurring operating requirements and not just crisis measures. Multinational operators may face competing national

priorities over restoration, scarce equipment, civil-military coordination, liability, and cost-sharing. Civilian operators retain civilian status, and civilian objects remain protected unless the applicable military-objective test is met (ICRC 1977, arts. 51–52, 57). These legal protections do not remove the need for advance arrangements on restoration priorities, repair allocation, and coordination across jurisdictions.

Resilience measures do not by themselves resolve the question of political response to state-linked sabotage. Attribution is rarely a single binary judgment. Protective measures, intelligence exchange, investigation, diplomatic consultation, and coordinated public communication can proceed while responsibility remains under assessment. Diplomatic, legal, and economic measures that impose greater costs require correspondingly stronger evidence and applicable legal grounds. Graduated response options can therefore reduce reliance on improvised decisions after individual incidents.

Six foreign-policy priorities follow:

- ▶ identify regional as well as national criticality through function-first cross-border assessments;
- ▶ establish trusted two-way mechanisms for threat information and operator knowledge;
- ▶ distinguish attribution of execution from attribution of enablement and sponsorship;
- ▶ develop graduated protective, investigative, diplomatic, and economic responses matched to evidentiary confidence;
- ▶ use regional cooperation to connect neighbouring systems while matching EU and NATO instruments to their respective functions; and
- ▶ plan with operators for sustained pressure, including multinational priority-setting and access to scarce repair capacity.

1. The changing physical threat environment

Physical threats to European critical infrastructure increasingly span the boundary between domestic security and foreign policy. Energy facilities, railways, ports, logistics hubs, telecommunications nodes, data centres, subsea infrastructure, and transport corridors can generate effects far beyond the physical location of an incident. The Council of the EU consequently identifies sabotage against critical infrastructure among the hybrid activities threatening the Union and explicitly recognises both state and non-state actors as potential sources of such activity (Council of the European Union 2026).

In July 2025, the EU described Russian hybrid campaigns as including sabotage, disruption of critical infrastructure, physical attacks, information manipulation, and other covert or coercive actions (Council of the European Union 2025). Research into post-2022 Russian operations has also documented extensive reliance on locally recruited and frequently criminally connected “disposable” agents. An ICCT-GLOBSEC study identified recurring criminal backgrounds among perpetrators, while a 2026 update found continued recruitment of individuals with no formal intelligence affilia-

tion for sabotage and other kinetic operations across Europe (Rekawek et al. 2025; Lanchès and Rewakew 2026).

This report distinguishes the wider physical threat environment from hybrid activity. The Council of the EU describes hybrid campaigns as coordinated harmful activities planned and carried out with malign intent, often through a combination of means designed to complicate detection and response; such tactics may be used by state or non-state actors (Council of the European Union 2026). Autonomous crime or extremism is not treated as hybrid solely because it crosses borders. It remains relevant where capabilities, information, vulnerabilities, or recruits intersect with state or proxy activity. Section 5 focuses on the state-linked and strategically coordinated part of this wider environment.

For each incident, the report separates four questions: actor, who executed the act; motive, the immediate purpose; linkage and enablement, including recruitment, direction, financing, supply, training, or information support and the confidence attached to those links; and effect,

Illustrative case: Homegrown infrastructure sabotage and networked extremism in Germany

Since 2011, actors using the *Vulkangruppen* label have claimed arson and sabotage attacks against electricity, railway, communications and industrial infrastructure in Germany. A March 2024 attack on electricity infrastructure supplying Tesla’s Grünheide factory interrupted production and affected surrounding facilities and households (BfV 2025).

The consequences became substantially larger on 3 January 2026, when high-voltage cables were deliberately set alight near Berlin-Lichterfelde. The resulting outage affected approximately 45,400 households and 2,200 businesses across southwest Berlin and disrupted district-heating provision (Berlin Senate 2026). A Vulkangruppe claimed responsibility. The BfV later regarded related statements published under the label as authentic, while cautioning that different structures may use the name; police reported no evidence at that stage of Russian responsibility (RBB 2026a, 2026b).

During the blackout, Kommando Angry Birds (KAB), a separate label previously associated with attacks on railway and electricity infrastructure, circulated a document advocating a wider network capable of coordinated infrastructure attacks (RBB 2026b). No public evidence establishes operational cooperation between KAB and the perpetrators of the Berlin attack.

including affected services, jurisdictions, markets, alliances, or political decisions. Foreign provenance, transnational diffusion, sponsorship, and state direction are treated separately.

Homegrown actors can target infrastructure autonomously for ideological purposes. Germany's Federal Office for the Protection of the Constitution, for example, assesses that so-called Vulkangruppen have conducted arson attacks against important infrastructure nodes since 2011 and places attacks of this kind within the violent left-wing extremist threat environment (BfV 2025). Criminal groups may likewise attack infrastructure for profit, to facilitate other crimes, or for coercive purposes without pursuing a geopolitical objective. In December 2024, German and Bulgarian authorities dismantled an organised group linked to 45 large-scale power-cable thefts across three German states. The cables were sold for profit, while their removal caused significant disruption to public construction sites (Eurojust 2024).

In the Berlin case, publicly available evidence is stronger on the apparent actor, immediate motive, and effects than on wider linkage. A domestically rooted extremist network may draw on transnational ideological or technical communities without serving a state. A criminal group may operate across borders without serving a state. Conversely, Russian operations have recruited criminals and other locally based agents as proxies (Rekawek et al. 2025; Lanchès and Rekawek 2026). Transnational activity alone does not establish foreign direction.

Digital information environments further weaken traditional organisational boundaries. EU-supported research has identified extremist activity across gaming and gaming-adjacent environments including Discord, Steam, Roblox, Reddit, Twitch, and other platforms (European Commission, Directorate-General for Migration and Home Affairs 2026). Sensitive information, technical knowledge, or targeting ideas obtained by one actor can consequently circulate through unrelated communities before being adopted by another. A useful distinction is between direct enablement, such as recruitment or tasking, and indirect enablement, where capabilities or information generated by one actor subsequently become available to autonomous actors without organisational contact. Foreign provenance of information does not in itself establish foreign direction of the eventual attack.

Technological diffusion can similarly separate international capability transfer from physical movement. The European Commission's 2026 firearms proposal specifically addresses the illicit creation,

acquisition, possession, and dissemination of digital blueprints for 3D-printed firearms (European Commission 2026b). The infrastructure-security relevance is broader than firearms themselves: designs and technical knowledge can cross borders digitally while capability generation remains local. Conflict experience can travel in similar ways. Reporting by the *Financial Times* in August 2026 documented concerns that individuals linked to Colombian organised crime had sought service in Ukraine in order to acquire contemporary drone-warfare expertise for later use at home (Daniels, Miller, and Dyer 2026). These cases illustrate a wider process through which information, technical capability, operational experience, and potentially matériel can diffuse beyond the conflict or community in which they originated.

Illustrative precedent: Operation Dragonfire

In the mid-1990s, U.S. authorities infiltrated an international network seeking to smuggle 2,000 fully automatic AK-pattern weapons from China through the Port of Oakland. ATF records confirm the 2,000-weapon transaction and the involvement of Chinese co-conspirators (ATF 2016). Contemporary reporting on the federal investigation identified Norinco and Poly Technologies as state-controlled or military-linked Chinese arms exporters and reported active participation by senior Norinco personnel. The traffickers understood that the weapons could enter the U.S. criminal market, including gang use (Paddock and Ostrow 1996). U.S. officials did not establish that the Chinese government had directed or sanctioned the operation. The case nevertheless provides a historical precedent for state-linked commercial structures intersecting directly with illicit criminal arms markets.

The resulting environment is better understood as an **overlapping threat ecosystem** than as a ladder running from criminality through extremism to state sabotage. For foreign-policy purposes, the central issue is not simply who commits an attack, but how capabilities travel and how locally executed disruption creates consequences across jurisdictions.

2. Legacy protection regimes, cross-border exposure, and modern infrastructure needs

European infrastructure protection remains organised primarily through national jurisdiction even where the infrastructure itself forms part of a wider regional system. The CER Directive establishes common requirements for national risk assessments, identification of critical entities, and resilience measures. It requires critical-entity risk assessments to consider cross-border risks and dependencies on services located in neighbouring Member States and third countries (European Parliament and Council 2022, art. 12). CER also defines ‘critical entities of particular European significance’ where an identified critical entity provides the same or similar essential services to or in six or more Member States (art. 17). That threshold does not cover all regionally important dependencies involving fewer states.

The underlying governance problem nevertheless remains: responsibility is predominantly national while criticality is increasingly regional. Electricity grids, pipelines, ports, telecommunications links, logistics chains, and transport corridors cross national boundaries or support users in several countries. Multinational firms may own or operate assets across multiple jurisdictions, while the failure of an asset in one country can impose disproportionate costs on another. Military mo-

bility adds a further strategic dimension because civilian transport and logistics nodes can acquire importance to allied reinforcement beyond their normal commercial function.

National risk assessments and protection priorities therefore do not necessarily capture the full geographic distribution of risk. States may differ in threat perception, in their assessment of the significance of particular infrastructure, and in the threshold at which an incident is treated as criminality, terrorism, hybrid interference, or hostile-state sabotage. These differences influence not only physical protection but also the willingness to share intelligence, attribute responsibility publicly, activate European mechanisms, or impose foreign-policy consequences.

The EU has progressively recognised this mismatch. The 2024 Critical Infrastructure Blueprint establishes an EU-level coordination framework for incidents with significant cross-border relevance and seeks to improve shared situational awareness, information exchange, public communication, and coordination among affected states (Council of the European Union 2024). The Preparedness Union Strategy similarly calls for more regular EU exercises, stronger external

Illustrative precedent: the 2006 European electricity disturbance

On 4 November 2006, a planned disconnection of a high-voltage line in northern Germany to permit a ship to pass along the River Ems contributed to a cascading disturbance in the continental European power system. The interconnected network separated into three areas and power supply was disrupted for more than 15 million European households (UCTE 2007). European regulators subsequently identified shortcomings in coordination and cooperation among transmission-system operators as an important lesson from the incident (ERGEG 2007). The incident was not sabotage. Precisely for that reason, it demonstrates the structural point: a geographically limited intervention in one national network can generate immediate consequences throughout an interconnected European system.

partnerships, and deeper EU-NATO cooperation (European Commission and High Representative 2025a). These mechanisms remain most useful, however, when governments have already identified which nationally located assets carry wider regional significance.

Cross-border coordination is complicated by national thresholds and jurisdiction. Under CER, each Member State identifies critical entities under Article 6 and may apply thresholds under Article 7. Maritime infrastructure adds a separate jurisdictional issue. A submarine cable may cross territorial seas and the high seas, while the operational effect of a break is not determined by the maritime zone in which it occurs. Coastal-state enforcement jurisdiction is more limited outside territorial waters and varies by maritime zone, legal basis, and conduct (Sari 2025, 22). Pillai's 2023 analysis identified Italy, the Netherlands, and Poland as relatively reluctant to share information on critical infrastructure, particularly subsea cables, and Austria, Hungary, and Italy as more reluctant to involve the Union in countering hybrid threats, partly because of lower threat perception (Pillai 2023). Response thresholds also remain contested. A cable or pipeline cut may fall below the armed-attack threshold, and a multi-state asset can complicate identification of the victim state for self-defence purposes (Sari 2025, 34–35; Olech 2025, 135). Article 222 TFEU, Article 42(7) TEU, and NATO Article 5 have different triggers and consequences. The EU does not have NATO's integrated military command or Article 5 framework; Member States retain national capabilities and mutual-assistance obligations under Article 42(7) TEU (Fazio 2025; NATO 1949). The Preparedness Union Strategy links EU preparedness to solidarity under Article 222 TFEU (European Commission and High Representative 2025a).

Regional criticality mapping should start from functions and then trace the assets, substitute routes, spare capacity, operators, and dependencies needed to sustain them. This captures both substitutable nodes and assets that become critical when alternatives are unavailable. The assessments should inform bilateral and regional security planning, exercises, and protection priorities.



3. Public-private coordination

Much of Europe's critical infrastructure is privately owned or operated, while commercial operators may lack either the capabilities or incentives to invest against low-probability, high-impact security threats (Pillai 2023). European experts rank a disruptive hybrid strike on critical infrastructure as both the most likely and among the most impactful risks facing the Union in 2026, on the reasoning that coordinated disruption would divide political resolve rather than achieve military defeat (Anghel and Spatafora 2026). Europe's underwater network of cables and pipelines was not designed with hybrid warfare threats in mind (Olech 2025, 149). The relevant capabilities are split between the public and private sectors. Operators hold detailed knowledge of assets, technology, dependencies, supply chains, and restoration requirements; public authorities hold the wider threat picture, regulatory and security powers, crisis coordination, and state capabilities. European and NATO frameworks accordingly involve operators in risk assessment, planning, information sharing, exercises, and crisis response (Niinistö 2024, 95–96; European Commission and High Representative 2025a; NATO 2026).

Threat Awareness

This relationship begins with threat awareness. The CER Directive obliges Member States to make relevant elements of national risk assessments available to identified critical entities, where relevant through their single points of contact, and to ensure that the information provided assists operators in carrying out their own risk assessments and in taking measures to ensure their resilience (European Parliament and Council 2022, art. 5(3)). At Union level, the Critical Entities Resilience Group provides a forum for exchanging information and good practice (European Parliament and Council 2022, art. 19), while the Hybrid Fusion Cell facilitates information-sharing between Member States on hybrid threats (Pillai 2023). In practice, this requires authorities to translate strategic threat information into material operators can use, while operators provide asset-level knowledge of vulnerabilities, dependencies, and operational conditions.

Illustrative practice: sharing classified threat information with Norwegian operators

Following the Nord Stream sabotage and heightened concern over offshore energy infrastructure, Norway brought Equinor and Gassco under relevant provisions of the Security Act. The Norwegian government stated that selected employees could consequently receive security clearances and access classified information concerning security threats (Government of Norway 2022). The arrangement preserved operators' responsibility for security while creating a mechanism through which sensitive state threat assessments could reach personnel responsible for strategically significant private infrastructure. It provides a practical example of how governments can narrow the information gap between national security authorities and operators.

Finland uses a different institutional model of public-private preparedness. Its National Emergency Supply Organisation brings authorities, companies, and organisations together through sectors and industry-managed pools that plan operational preparedness and identify firms critical to security of supply. Legislation that entered into force in 2026 retained these cooperation structures as the National Emergency Supply Agency became a government agency (National Emergency Supply Agency 2026a, 2026b). Sweden's historical K-company system and Finland's sector-and-pool model differ in form, but both formalise operator relationships before crisis (Malmberg et al. 2023; National Emergency Supply Agency 2026a, 2026b).

Site Protection

The same division of responsibilities applies to site protection. Article 13(1) requires Member States to ensure that critical entities take appropriate and proportionate technical, security and organisational measures. These include adequate physical protection of premises and critical infrastructure through means such as perimeter monitoring, detection equipment and access controls (European Parliament and Council 2022, art. 13(1)(b)), as well as employee security management, including procedures for background checks in accordance with Article 14 (art. 13(1)(e)). Commission guidelines adopted under Article 13(5) in July 2026 provide operational guidance for each of these categories (European Commission 2026a). Personnel vetting is one relevant counter-proxy measure: Russian operations have increasingly relied on criminal networks and local recruits for physical attacks while preserving deniability (Beznosiuk and Dixon 2026; Rekawek et al. 2025; Lanchès and Rekawek 2026). Responsibility nevertheless does not rest with the operator alone. Authorities contribute the wider threat picture, security guidance and, where necessary, other state security capabilities, while operators translate that information into site-specific protection based on their knowledge of facilities, personnel, vulnerabilities and operational dependencies. Current NATO resilience guidance accordingly calls for joint or coordinated risk assessments, continuous threat-information sharing and clearly defined public, private and military responsibilities for infrastructure protection (European Parliament and Council 2022, arts. 12–13; NATO 2026).

Incident response

Incident response similarly relies on a two-way relationship. Article 15 requires Member States to ensure that critical entities notify the competent authority, without undue delay, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services, with a reciprocal duty on the authority to provide relevant follow-up information. Where disruptions have significant cross-border relevance, including cases affecting two or more Member States, the Council blueprint provides a framework for Union-level coordination where the relevant conditions for escalation are met (Council of the European Union 2024). Operators provide the initial asset-level information on disruption and its operational effects, while competent authorities aggregate that information, assess wider security and cross-border implications and coordinate

with other state authorities and affected Member States (European Parliament and Council 2022, art. 15; NATO 2026). Effective response therefore depends on rapid two-way information exchange and mechanisms that allow public and private experts to develop a common situational picture rather than on notification alone. This becomes particularly important in hybrid incidents, where the difficulty of identifying the aggressor can weaken deterrence and turn an initially operational disruption into a political and security problem (Pillai 2023).

Recovery and repair capacity

Recovery forms part of the Article 13 resilience obligation, and resilience contributes not only to mitigating vulnerabilities and recovering from attack but also to deterring adversaries by denial (Sari 2025, 12). Recovery combines operator responsibility with public coordination: critical entities remain responsible for continuity arrangements and restoring essential-service provision, but major or simultaneous disruptions can require capabilities beyond those available to an individual operator, including coordination across sectors and jurisdictions, emergency logistical support and mobilisation of additional repair capacity. NATO guidance therefore recommends that public authorities and private infrastructure providers jointly plan response, recovery and repair requirements in advance rather than develop such arrangements only after a crisis occurs (European Parliament and Council 2022, art. 13(1)(d); NATO 2026).

Subsea infrastructure illustrates the scale of this challenge. The Niinistö report recommends an EU governance system for submarine cable infrastructure, including a common EU maintenance and repair fleet, and identifies cooperation with NATO as a means of sharing the costs of improved subsea preparedness (Niinistö 2024, 99–100). The EU Action Plan on Cable Security identifies maintenance and repair vessels as a bottleneck in systemic or simultaneous attacks and sets an objective of moving towards an EU cable vessels reserve fleet (European Commission and High Representative 2025b). A standing Union-wide reserve fleet remains an objective rather than an operational capability. Simultaneous failures could also create competing demand for specialist crews, transformers, spares, and replacement equipment. Advance arrangements can define access and prioritisation rules for such scarce capacity.



Information sharing and attribution

Despite this developing framework, information-sharing remains a central weakness. The institutional architecture is nevertheless asymmetric. Operator obligations under the Directive are backed by dedicated supervisory and enforcement provisions, including Articles 21 and 22, whereas Article 5(3)'s corresponding obligation on Member States to provide useful risk information is not accompanied by a comparable sector-specific supervisory mechanism. Persistent trust deficits may further constrain information-sharing. Pillai's 2023 assessment, for example, found that information exchange functioned comparatively well at staff level between the EU and NATO but was more constrained among national governments, limiting what could ultimately reach operators (Pillai 2023). Attribution adds a further evidentiary challenge. Nearly two thirds of damage to submarine cables is accidental in origin, making robust situational awareness necessary to distinguish accidents from deliberate attacks; compelling evidence is also required before malicious acts can be attributed to state or non-state perpetrators and those perpetrators held to account (Sari 2025, 11). Sari accordingly recommends that EU Member States and NATO allies reinforce mechanisms for information sharing and for the individual and collective attribution of hybrid threats (Sari 2025, 36). The wider litera-

ture similarly calls for joint exercises and real-time information-sharing initiatives to be expanded to improve threat detection and response (Olech 2025, 154).

Exercises

The challenge in crisis exercises is therefore fragmentation rather than absence. The Preparedness Union Strategy acknowledges that the EU crisis management toolbox is fragmented across institutions, services and agencies and suffers from sectoral and cross-border coordination gaps. It also observes that large-scale exercises are often fragmented and underutilised and do not consistently involve all relevant civilian and military stakeholders (European Commission and High Representative 2025a). The Niinistö report had proposed that the Union adopt an EU-wide exercise policy promoting shared approaches across sectors and institutions, supported by a centrally accessible exercise knowledge hub (Niinistö 2024, 69–70). The Strategy takes this forward by committing the Commission and the High Representative to organise regular Union-wide cross-sectoral preparedness exercises to test decision-making, coordination and operational response, expressly including within the remit of Article 42(7) TEU and Article 222 TFEU (European Commission and High Representative 2025a). The wider literature likewise calls for more frequent joint training and exercises between the EU and NATO (Pillai 2023).

4. Sustaining essential services under prolonged attack

The CER Directive, the Critical Infrastructure Blueprint, and the Preparedness Union Strategy provide all-hazards resilience and coordinated crisis-response frameworks. They do not establish a comprehensive operating regime for multinational infrastructure providers under prolonged armed attack (European Parliament and Council 2022; Council of the European Union 2024; European Commission and High Representative 2025a). Civil-military coordination, prioritisation, liability, insurance, cost-sharing for hostile-state damage, repair capacity, and cross-border direction remain governed by other instruments or national arrangements. Since 2022, Ukraine's energy system has operated under repeated strikes on

generation, transmission, and district heating, with repair and continuity becoming recurring operating requirements (IEA 2024).

International humanitarian law continues to distinguish civilian objects from military objectives. In 2022, a senior Russian official stated that Western commercial satellites supporting Ukrainian military operations could become 'legitimate' targets (RFE/RL 2022). Lawful targetability does not follow from such statements. A civilian asset may be attacked only if, in the circumstances at the time, it meets the military-objective test; support for national resilience or defence does not by itself make the operator as a whole or its workforce

Illustrative case: Gulf desalination plants, power infrastructure and data centres in the 2026 Iran war

Since the outbreak of war between the United States and Israel and Iran on 28 February 2026, water infrastructure in the Gulf has been drawn directly into the conflict. As of September 2026, the public record contains both confirmed damage and contested claims of deliberate targeting. Desalination facilities in Kuwait and the United Arab Emirates suffered damage during missile and drone attacks early in the war; subsequent incidents in Bahrain and Iran involved reported attacks whose attribution or deliberate targeting was contested in some cases (CSIS 2026; The National 2026). On 7 March, Iran accused the United States of striking a desalination plant on Qeshm Island, cutting supply to some 30 villages; the United States and Israel denied responsibility. The following day, Bahrain reported that an Iranian drone had struck one of its desalination plants (Shehabi 2026; The National 2026).

Foreign commercial exposure is also visible in the Gulf cases. In Kuwait, technical and emergency teams were dispatched after a service building at a power and desalination plant was hit on 29 March, killing an Indian worker (Al Jazeera 2026a). Iranian statements have explicitly threatened regional energy, information, and telecommunications infrastructure associated with American interests if Iranian power plants are attacked; earlier in the conflict, Amazon Web Services confirmed that two of its data centres in the UAE were directly struck and a third in Bahrain was damaged by a nearby drone strike (Al Jazeera 2026b). The public record therefore includes both physical damage to foreign-operated assets and threats framed around commercial affiliation.

lawful targets. Civilians remain protected against direct attack unless and for such time as they directly participate in hostilities, while attacks on military objectives remain subject to distinction, proportionality, and precautions (ICRC 1977, arts. 51–52, 57). That legal baseline does not answer the governance questions above, and those questions become more consequential as disruption becomes sustained.

Multinational operators may also face competing national instructions over repair crews, spare equipment, traffic prioritisation, restoration sequencing, and continuity decisions. Advance arrangements can specify which public authority sets priorities, how conflicting instructions are reconciled, and what operational discretion a provider retains when critical capabilities are distributed across several jurisdictions.



5. Transferable lessons and European foreign-policy options

Europe already possesses much of the institutional architecture required to strengthen infrastructure resilience. The principal challenge is to make national, regional, EU, and NATO mechanisms operate across the same boundaries as the infrastructure and threat ecosystems they are intended to manage. The Preparedness Union Strategy describes preparedness as both a national and shared European responsibility, while NATO's 2026 guidance explicitly recommends cooperation with neighbouring states and transnational firms to identify cascading risks in shared infrastructure and supply chains (European Commission and High Representative 2025a; NATO 2026).

Nordic experience is useful not because it constitutes a single model, but because longstanding infrastructure integration has generated practical arrangements for cross-border cooperation. Electricity preparedness provides a particularly useful example.

Six foreign-policy priorities follow. Near-term measures include cross-border risk mapping, trusted information exchange, clearer attribution practices, and pre-agreed crisis communication. Shared repair-capacity arrangements, consequence frameworks, and continuity planning

under sustained pressure require deeper legal, financial, and political commitments.

First, identify regional as well as national criticality. Member States, regional groupings, and operators should conduct function-first cross-border assessments covering vital functions, dependencies, substitutes, alternative routes, and single points of failure. The results should inform bilateral security dialogues, regional exercises, and protection priorities.

Second, connect foreign-policy and security assessments more effectively with operators. Member States should establish trusted channels for relevant information on hostile-state activity, proxy recruitment, and transnational threats, while operators provide asset-level information on vulnerabilities, dependencies, supply constraints, and restoration needs. NATO recommends secure channels for classified information and, where appropriate, security clearances for essential private-sector personnel (NATO 2026). Norway provides a precedent for secure threat exchange, while Finland embeds operator participation through standing preparedness structures (Government of Norway 2022; National Emergency Supply Agency 2026a, 2026b).

Illustrative practice: NordBER and Nordic electricity preparedness

NordBER brings together electricity authorities and transmission-system operators across the Nordic countries for information exchange, exercises, and preparedness coordination. Sweden's electricity risk-preparedness arrangements require consultation with neighbouring competent authorities and transmission-system operators and record the use of NordBER exercises to test cross-border communication mechanisms (Swedish Energy Agency 2026a, 2026b). Recent Nordic analysis nevertheless concludes that this architecture was designed largely for a pre-2022 risk environment and requires adaptation to scenarios involving deliberate, simultaneous, and cross-border disruption (Nordic Energy Research 2026). The lesson is therefore institutional rather than celebratory: permanent regional machinery provides a platform that can be adapted as the threat environment changes.

Third, distinguish attribution of execution from attribution of enablement and sponsorship.

Governments should state separately what is known about the physical perpetrator, capability provenance, enablement or sponsorship, and strategic effect. Public attribution should distinguish confirmed facts, official assessments, and unresolved inference. Protective and political measures can then be calibrated to the evidentiary picture.

Fourth, develop graduated and coordinated foreign-policy consequences.

The EU framework recognises that not every measure in a coordinated response requires responsibility to be assigned publicly and that measures can be calibrated to the degree of certainty available (Council of the European Union 2022, para. 18). While attribution is developing, governments can coordinate protective measures, intelligence exchange, diplomatic consultation, law-enforcement investigation, exposure of hostile tactics where evidence permits, and public communication. Where a perpetrator can be identified with a high degree of certainty, the framework provides for proportionate diplomatic, political, economic, strategic-communication and, where appropriate, restrictive measures (Council of the European Union 2022, paras. 14–15; Council of the European Union 2026). These measures can be organised in a pre-agreed response ladder.

Fifth, use regional cooperation as an operational layer with a clearer division of labour.

Regional formats can connect neighbouring preparedness systems, operators, and technical expertise around shared infrastructure. EU mechanisms add regulatory, financial, and Union-wide coordination capacity. NATO provides the principal collective-defence framework and relevant functions in deterrence, military mobility, and civil-military resilience. Interfaces for escalation, information exchange, exercises, and crisis communication should be agreed in advance (European Commission and High Representative 2025a; NATO 2026).

Sixth, plan for sustained pressure. Member States should determine with operators and neighbouring governments which functions and assets receive priority protection, who sets restoration priorities for multinational providers, how conflicting instructions are reconciled, how scarce repair capacity is allocated under simultaneous demand, and how liability, insurance, and hostile-state damage are handled. Regional exercises should test these allocation and decision rules. The CER framework provides the peacetime baseline but not a comprehensive wartime oper-

ating regime. Planning should draw on Ukraine's experience and the Gulf case.

Europe cannot remove every physical vulnerability from extensive civilian infrastructure networks. It can, however, make cascading effects more difficult to generate, improve the speed and credibility of attribution, coordinate recovery and political response more effectively, and reduce the ability of hostile actors to exploit gaps between national jurisdictions. Doing so requires treating critical-infrastructure resilience not solely as a responsibility of regulators, police, or defence establishments, but increasingly as an element of European foreign and security policy.

References

- Al Jazeera. 2026a. "Iranian Attack Damages Kuwait Power and Desalination Plant, Kills Worker." March 30, 2026.
- Al Jazeera. 2026b. "Kuwait Desalination Plant, Oil Refinery Hit by Missile and Drone Strikes." April 3, 2026.
- Anghel, Veronica, and Giuseppe Spatafora. 2026. "Global Risks to the EU in 2026: What Are the Main Conflict Threats for Europe?" *EUISS Commentary*, January 20, 2026.
- Berlin Senate. 2026. "Stromausfall im Berliner Südwesten." January 3, 2026.
- Beznosiuk, Maksym, and William Dixon. 2026. "How Russia's Hybrid Warfare Will Escalate in 2026 and What Europe Must Do?" *GLOBSEC Commentary*, January 13, 2026.
- BfV (Bundesamt für Verfassungsschutz). 2025. *Verfassungsschutzbericht 2024*. Cologne: Bundesamt für Verfassungsschutz.
- Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). 2016. "Operation Dragonfire." Last updated September 22, 2016.
- Council of the European Union. 2022. "Council Conclusions on a Framework for a Coordinated EU Response to Hybrid Campaigns." June 21, 2022.
- Council of the European Union. 2024. *Recommendation of 25 June 2024 on a Blueprint to Coordinate a Response at Union Level to Disruptions of Critical Infrastructure with Significant Cross-Border Relevance*. C/2024/4371. *Official Journal of the European Union*, July 5, 2024.
- Council of the European Union. 2025. "Hybrid Threats/Russia: Statement by the High Representative on Behalf of the EU Condemning Russia's Persistent Hybrid Campaigns against the EU, Its Member States and Partners." July 18, 2025.
- Council of the European Union. 2026. "Council Adopts Conclusions on Advancing the EU's Capacity to Counter Hybrid Threats." March 16, 2026.
- CSIS (Center for Strategic and International Studies). 2026. "Could Iran Disrupt the Gulf Countries' Desalinated Water Supplies?" March 19, 2026.
- Daniels, Joe, Christopher Miller, and Geoff Dyer. 2026. "Colombian Narcos Head to Ukraine for Drone Expertise." *Financial Times*, August 6, 2026.
- EREGG (European Regulators' Group for Electricity and Gas). 2007. *The Lessons to Be Learned from the Large Disturbance in the European Power System on 4 November 2006*. E06-BAG-01-06. Brussels: EREGG.
- Eurojust. 2024. "Criminal Group Disrupting Public Services by Stealing Power Cables Arrested." December 18, 2024.
- European Commission. 2026a. "Guidelines on the Application of Article 13(5) of Directive (EU) 2022/2557 on the Resilience of Critical Entities." Communication C/2026/4730. *Official Journal of the European Union* C, C/2026/3712, July 13, 2026.
- European Commission. 2026b. "Commission Proposes New Rules to Combat the Trafficking of Illicit Firearms." Directorate-General for Migration and Home Affairs, February 26, 2026.
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy. 2025a. *Joint Communication on the European Preparedness Union Strategy*. JOIN(2025) 130 final. Brussels, March 26, 2025.
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy. 2025b. *Joint Communication on an EU Action Plan on Cable Security*. JOIN(2025) 9 final. Brussels, February 21, 2025.

European Commission, Directorate-General for Migration and Home Affairs. 2026. “Streaming, Chatting, Modding: A Brief Exploration of Extremist Activities on Gaming and Gaming-Adjacent Platforms.” EU Knowledge Hub on Prevention of Radicalisation, March 11, 2026.

European Parliament and Council of the European Union. 2022. *Directive (EU) 2022/2557 of 14 December 2022 on the Resilience of Critical Entities*. Official Journal of the European Union L 333: 164–198.

Fazio, Federica. 2025. “The EU’s Mutual Defence Clause: Legal and Strategic Considerations on Article 42(7) TEU in Light of the War in Ukraine.” *Nordic Journal of European Law* 8 (3): 1–30. <https://doi.org/10.36969/njel.v8i3.28035>.

Government of Norway. 2022. “Prime Minister Jonas Gahr Støre Address to the Storting.” Office of the Prime Minister, October 28, 2022.

IEA (International Energy Agency). 2024. *Ukraine’s Energy Security and the Coming Winter*. Paris: International Energy Agency.

International Committee of the Red Cross (ICRC). 1977. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), Articles 51–52 and 57. June 8, 1977.

Lanchès, Julian, and Kacper Rekawek. 2026. “More of the Same: Russia’s Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare Revisited.” International Centre for Counter-Terrorism, February 23, 2026.

Malmberg, Pär, Jan Ottosson, Martin Eriksson, and Olle Jansson. 2023. “The Role of Industry in Sweden’s Total Defence: Past, Present, and Future.” National Preparedness Commission, February 21, 2023.

National Emergency Supply Agency. 2026a. “Public–Private Partnership.” Accessed September 16, 2026.

National Emergency Supply Agency. 2026b. “New Law Supports the Strengthening and Financial Base of Security of Supply – The National Emergency Supply Agency Became a Government Agency on 1 April.” April 2, 2026.

NATO. 1949. The North Atlantic Treaty. Article 5. Washington, DC, April 4, 1949.

NATO. 2026. *Guidance for Enhancing Public-Private Cooperation for Resilience*. Brussels: North Atlantic Treaty Organization, July 16, 2026.

Niinistö, Sauli. 2024. *Safer Together: Strengthening Europe’s Civilian and Military Preparedness and Readiness*. Report by the Special Adviser to the President of the European Commission. Brussels: European Commission.

Nordic Energy Research. 2026. *Energy Security in the Nordics*. Oslo: Nordic Energy Research.

Olech, Aleksander. 2025. “Hybrid Threats to Critical Infrastructure in the European Union: Selected Hybrid CoE Analyses.” *Terrorism: Studies, Analyses, Prevention*, special edition: 133–158. <https://doi.org/10.4467/27204383TER.25.017.21520>.

Paddock, Richard C., and Ronald J. Ostrow. 1996. “U.S. Agents Say Chinese Tanks, Rockets Offered.” *Los Angeles Times*, May 24, 1996.

Pillai, Helmi. 2023. *Protecting Europe’s Critical Infrastructure from Russian Hybrid Threats*. London: Centre for European Reform.

RBB. 2026a. “Anschlag aufs Berliner Stromnetz: ‘Vulkangruppe’ weist Russland-Spekulationen zurück.” January 7, 2026.

RBB. 2026b. “‘Manifest’ aufgetaucht: Wie Linksextremisten im Untergrund agieren.” January 16, 2026.

Rekawek, Kacper, Julian Lanchès, Maria Zotova, and Donald Bowser. 2025. *Russia’s Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare in Europe*. The Hague and Bratislava: International Centre for Counter-Terrorism and GLOBSEC.

RFE/RL. 2022. “Russian Official Says Western Commercial Satellites Could Become ‘Legitimate’ Targets.” Radio Free Europe/Radio Liberty, October 27, 2022.

Sari, Aurel. 2025. *Protecting Maritime Infrastructure from Hybrid Threats: Legal Options*. Hybrid CoE Research Report 14. Helsinki: European Centre of Excellence for Countering Hybrid Threats.

Shehabi, Manal. 2026. "War on Iran: The Dangers of Attacking Water Desalination Plants in the Gulf." Arab Center Washington DC, April 28, 2026.

Swedish Energy Agency. 2026a. "Risk Preparedness in the Electricity Sector." Eskilstuna: Swedish Energy Agency.

Swedish Energy Agency. 2026b. *National Risk-Preparedness Plan for Sweden's Electricity Supply*. Version 6. Reference no. 2024-009023. Adopted January 21, 2026. Eskilstuna: Swedish Energy Agency.

The National. 2026. "Iran's Strike on Bahrain Desalination Plant Brings Gulf Water Security into Focus." March 8, 2026.

UCTE (Union for the Coordination of Transmission of Electricity). 2007. *Final Report: System Disturbance on 4 November 2006*. Brussels: UCTE.

