

GLOBSEC
IDEAS SHAPING THE WORLD

GeoTech Center

Protecting critical infrastructure from cyber threats

Alexandr Burilkov, Diana Sarah Ondrejkovičová

Authors:

Alexandr Burilkov, Diana Sarah Ondrejkovičová

November 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.

GLOBSEC
IDEAS SHAPING THE WORLD

GeoTech Center

Sweden
Sverige

Executive Summary

Europe should safeguard essential services even when cyber defences fail. The attacks on KA-SAT and Polish energy facilities exposed risks to communications and industrial operations. PHP2Shell, XZ Utils and the CrowdStrike outage revealed a different vulnerability: software shared across sectors and borders. A failure upstream can disable services in several countries at once, beyond the control of any single operator.

Continuity of service is the immediate test of cyber defence. During the Polish attacks, industrial processes were interrupted, yet household heating continued. Authorities should require operators to demonstrate minimum service levels during prolonged disruption, with manual fallbacks, isolation procedures and tested restoration. These capabilities reduce the benefits of an attack and can strengthen deterrence by denial.

European regulation needs an operational counterpart. NIS2, DORA and the Cyber Resilience Act establish important security obligations, but incident reports alone cannot produce the shared situational awareness needed during a crisis. Finland's information-sharing arrangements, Sweden's consolidation of cyber functions and Nordic-Baltic cooperation offer practical foundations for linking private operators, national authorities and EU response mechanisms.

Hostile cyber operations should carry tangible consequences. The EU has used public attribution and sanctions, while Operation Eastwood temporarily disrupted infrastructure supporting a pro-Russian denial-of-service network. Governments should combine technical evidence with diplomatic, legal and law-enforcement action. Narrowly scoped offensive cyber operations also have a role when objectives, legal authority and expected effects are clear.

Five priorities for European governments:

- Map essential functions and upstream dependencies, including shared software, cloud services, satellite communications and remote-maintenance access.
- Test continued service under prolonged disruption, including manual operation, alternative systems and competing demands for recovery resources.
- Turn incident-reporting duties into trusted two-way information exchange between authorities, operators and security providers.
- Prepare regional response procedures, starting with Nordic–Baltic cooperation, alongside EU mechanisms, agreeing technical assistance, evidence sharing and crisis communication in advance
- Impose costs through coordinated attribution, sanctions, law enforcement and narrowly scoped offensive cyber operations, and judge them by observable effects.

1. Introduction

The protection of critical infrastructure in Europe should be organised around the continuity of essential services during sustained cyber disruption. Governments and operators need to know which services must continue, which external suppliers are critical, and how an incident will be managed across jurisdictions. The report examines publicly documented cases of espionage and pre-positioning, attempted destructive activity against industrial systems, communications disruption, software vulnerabilities and supply-chain compromise, alongside diplomatic and law-enforcement responses. It assesses each episode in terms of access, observed effects, continuity, attribution and response.

The cases were selected to illustrate distinct mechanisms of exposure and response, using public official or technical documentation. They are neither a representative sample of European cyber incidents nor an inventory of the most prevalent threats: ransomware, for example, remains prominent in threat statistics but is not examined as a separate vignette here. The United States-focused Volt Typhoon advisory is included as evidence of a pre-positioning method potentially relevant to European infrastructure.

The European Union Agency for Cybersecurity (ENISA) published its 2026 threat assessment, identifying ransomware as the most impactful short-term cyber threat. The assessment also describes politically motivated distributed denial-of-service (DDoS) attacks and cyberespionage affecting public administration and essential services (ENISA, 2026b). However, the number of attacks and intrusions is not a reliable proxy for disruption to essential services. The report therefore distinguishes between access, disruption, recovery, and attribution.

ENISA's 2026 threat landscape also describes the use of artificial intelligence (AI) in malicious activity (ENISA, 2026b). The October PHP2Shell disclosure illustrates a related development: researchers at Calif, OpenAI and Wiz used AI-assisted methods to identify critical flaws in PHP, a widely deployed software runtime (PHP Foundation, 2026). The case raises immediate questions about how quickly maintainers, suppliers and essential-service operators can discover exposure, coordinate fixes and prevent service interruption.

Volt Typhoon

A February 2024 multinational advisory assessed that actors associated with the China-linked Volt Typhoon campaign had maintained access to United States critical-infrastructure networks and could use that access for disruptive activity in a future crisis (CISA et al., 2024). The relevance for Europe lies in the method: long-term access to civilian systems can create options for interference before a crisis is apparent.

KA-SAT

The EU reported that a cyberattack on Viasat's KA-SAT service shortly before Russia's full-scale invasion of Ukraine in February 2022 disrupted satellite communications for users in Ukraine and EU member states, and it publicly attributed the operation to Russia (Council of the EU, 2022). Given the importance of satellite communications for civilian and military users, demonstrated since by Ukrainian forces' reliance on Starlink, the attack is a warning of potential cyber disruptions, even as the EU seeks to develop autonomy in the field, including through Eutelsat OneWeb and the planned IRIS^2 constellation.

2. Deterrence by denial

Deterrence by denial works when an adversary expects its objective to be unattainable (Nye, 2017). Network segmentation, access controls, monitoring and software maintenance can make disruption harder, while continuity arrangements reduce the consequences if an intrusion succeeds. Those two effects can strengthen a denial posture, but the immediate policy test is operational: whether essential services continue, destructive actions are blocked and affected systems can be restored. It should be noted that public incident reports rarely reveal the decisions of actors who chose not to attack, so claims about deterrence remain inferential (Bendiek and Hemmelskamp, 2025).

The cases in this report illustrate that test in different ways. The Polish energy attacks provide a direct test of defensive intervention and continuity. The PHP2Shell and XZ Utils episodes expose vulnerabilities in shared software upstream of critical operators (PHP Foundation, 2026; CERT-EU, 2024). A defective CrowdStrike update demonstrates that these same dependencies can interrupt services without any adversary (CrowdStrike, 2024). Together the cases justify protection and continuity measures independent of any claim that a particular attacker was deterred.

Attacks on Polish energy infrastructure (December 2025)

CERT Polska documented coordinated destructive cyberattacks on 29 December 2025 against more than 30 wind and solar installations, a manufacturing firm and a large combined heat-and-power (CHP) facility supplying nearly 500,000 customers. Communications at renewable installations were disrupted without stopping electricity generation; endpoint protection blocked an attempted destructive malware deployment at the large CHP plant. A separate, smaller CHP installation supplying roughly 50,000 residents was accessed through a misconfigured private mobile-network access point (APN). Its turbine and water-treatment process were interrupted, but operators prevented a loss of heat supply (CERT Polska, 2026a; 2026b). CERT Polska reported substantial infrastructure overlap with the activity cluster known as Static Tundra/ Berserk Bear. On 15 January 2026, Prime Minister Donald Tusk publicly linked the attacks to groups he said appeared connected to Russian services and announced additional cybersecurity measures (Government of Poland, 2026)

The Polish record shows that some planned destructive effects were prevented, others produced temporary interruption of industrial processes, and heat supply to consumers was maintained. That performance supports investment in detection, isolation and trained operator intervention, including for periods when an attacker retains access.

PHP2Shell (October 2026)

On 21 October 2026, the PHP project issued emergency releases for two critical remote-code-execution vulnerabilities (CVE-2026-109618 and CVE-2026-109619). Researchers at Calif, OpenAI and Wiz had found the flaws using AI-assisted methods and reported them; the PHP Foundation acknowledged that an underlying out-of-memory problem had been reported in 2024 but not resolved (PHP Foundation, 2026). Amazon observed attempted exploitation from 17 October, before public disclosure (Amazon, 2026). On 26 October, the US Cybersecurity and Infrastructure Security Agency (CISA) listed both flaws as known exploited vulnerabilities (CISA, 2026). By 29 October, Palo Alto Networks Unit 42 had confirmed reported attacks chaining PHP2Shell with privilege escalation against internet-exposed PAN-OS management interfaces (Palo Alto Networks Unit 42, 2026).

3. Deterrence by punishment: attribution, sanctions and law enforcement

Attribution is central to political and legal responses to malicious cyber activity, but it involves several distinct judgements. Technical investigations can link an intrusion to particular infrastructure, tools or patterns of activity, but identifying the organisations or individuals responsible requires further evidence. Establishing legal responsibility raises further questions (Egloff, 2020). European institutions have issued public attributions and imposed restrictive measures in response to specific operations. In May 2022, the EU attributed the KA-SAT attack to Russia. In January 2025, the Council listed three Russian military-intelligence officers in connection with cyber activity affecting Estonian ministries in 2020 (Council of the EU, 2022; Council of the EU, 2025a). These established an official position, and in the latter case, legal restrictions for those involved.

The EU's Cyber Diplomacy Toolbox, established in 2017 and supported by revised implementing guidelines in 2023, permits diplomatic measures and sanctions under the Common Foreign and Security Policy (Council of the EU, 2023). In March 2026, the Council sanctioned two China-based companies, two individuals and an Iran-based entity; July measures targeted additional Russia-linked persons and organisations associated with malicious cyber activity (Council of the EU, 2026a; 2026b). These measures imposed costs on identifiable targets, although any change in behavior depends on enforcement and on how exposed the targets are to those costs.

EU cyber sanctions impose asset freezes, travel restrictions and restrictions on supplying funds to listed parties; listing individuals or entities does not automatically establish the legal responsibility of a foreign state (Council Decision (CFSP) 2019/797). Law-enforcement interventions can seize assets, arrest participants and disable infrastructure. These are concrete disruptions, and they can contribute to deterrence by punishment when adversaries anticipate the costs (Nye, 2017).

Operation Eastwood (July 2025)

In July 2025, Europol and Eurojust coordinated Operation Eastwood against NoName057(16), a pro-Russian network conducting distributed denial-of-service attacks on Ukraine and countries supporting it. Participating states disrupted more than 100 systems and removed much of the network's central server infrastructure; private organisations including Shadowserver and abuse.ch contributed technical assistance (Europol, 2025; Eurojust, 2025). Independent monitoring subsequently reported renewed target lists and activity within days, illustrating that a successful takedown does not automatically end a campaign (Web-Performance, 2025).

European states should retain the option of narrowly scoped offensive cyber operations where they can prevent or interrupt serious ongoing harm, legal authority is established, the target and likely effects are sufficiently understood, and risks to third parties and escalation are manageable. The costs of revealing sensitive capabilities must also be weighed. Where they can achieve the intended effect, coordinated law enforcement and restrictive measures should normally be preferred. An offensive operation may otherwise be warranted on a case-specific basis (Bendiek and Bund, 2024).

4. Public-private roles in cyber deterrence

The European approach to cybersecurity relies on a division of responsibilities between public authorities and the operators of essential services. Many such services are owned, managed, or operated by private entities. These maintain their own networks, assessing vulnerabilities and managing incidents, while the role of national authorities is to regulate, supervise, and provide support (NATO, 2026; Serini, 2024).

NIS2 replaced the original Network and Information Systems Directive and covers eighteen sectors, with differentiated obligations for essential and important entities. It requires risk-management measures, incident notification and management accountability; the Digital Operational Resilience Act (DORA) specifies requirements and oversight for the financial sector (Directive (EU) 2022/2555, Arts 3, 20–23 and 34; Regulation (EU) 2022/2554, Arts 31–44). Yet incomplete and uneven national implementation continues to complicate oversight (European Commission, 2024).

Operators remain responsible for securing and restoring their systems, while national computer security incident response teams (CSIRTs) issue warnings, analyse incidents and assist under their mandates (NIS2, Arts 11 and 21). Because the relevant network logs and operational evidence usually originate with private operators, supervision and political attribution ultimately depend on information that public authorities cannot produce alone.

Three gaps remain especially consequential. First, mandatory notification presupposes that operators identify incidents; undetected compromises are absent from any reporting system. Second, national and sectoral practices have differed, and harmonised NIS2 definitions improve comparability only for reported incidents (NIS Cooperation Group, 2025; Schmitz-Berndt, 2023; Commission Implementing Regulation (EU) 2024/2690). Third, ENISA identified shortages of supervisory staff and budgets in some sectors and uneven maturity among national CSIRTs (ENISA, 2026a; ENISA, 2024).

Surge response likewise depends on private capabilities. The EU Cybersecurity Reserve, established by the Cyber Solidarity Act, draws on trusted private providers to supplement national capacity (Regulation (EU) 2025/38, Art. 14). For a multi-country incident, the availability of those specialists and their access to affected systems may matter more immediately than the existence of a regulatory duty on paper.

Public attribution depends on the same public–private evidence chain. For instance, private investigations contributed to attribution in the Bundestag, Democratic National Committee, WannaCry and NotPetya cases (Egloff, 2020). The German debate over proactive cyber disruption similarly places weight on reliable attribution before state action (Bendiek and Bund, 2024).

Information-sharing obligations do not themselves create trusted exchange. ENISA reported difficulties in cooperation concerning internet infrastructure and fragmented incident datasets (ENISA, 2024, p. 36). NIS2 asks member states to facilitate voluntary sharing, yet at least half of surveyed organisations in newly covered sectors were outside such arrangements (ENISA, 2025; NIS2, Art. 29). The Cyber Solidarity Act permits national cyber hubs to exchange detection data with private actors but does not make that exchange universal (Regulation (EU) 2025/38, Art. 4(3)).

Operators may also fear reputational damage and regulatory exposure from disclosure. Although NIS2 states that notification does not in itself increase liability, non-compliance with risk-management and notification duties can be sanctioned (NIS2, Arts 23 and 34). In a study of 320 listed companies in Germany, France and the United Kingdom, only 26 disclosed a current or previous cyber incident in their 2022 annual reports (Gauch et al., 2026).

Overlapping reporting obligations add friction. Depending on the incident, NIS2, DORA, the Critical Entities Resilience Directive and the General Data Protection Regulation may establish separate requirements, even where their substantive scopes are differentiated (DORA, Art. 1(2); NIS2, Art. 4; Directive (EU) 2022/2557, Art. 1(2); Regulation (EU) 2016/679, Art. 33). The Commission proposed simplification in 2025 (European Commission, 2025). Capacity is uneven, as 63% of small



and medium enterprises in ENISA's 2025 survey reported no cybersecurity assessment, compared with 24% of large enterprises (ENISA, 2025).

Finland offers a model for connecting statutory duties with trusted operational exchange. Its National Cyber Security Centre (NCSC-FI), within the Transport and Communications Agency Traficom, receives copies of NIS2 incident notifications while also accepting confidential voluntary reports and requests for CSIRT assistance (Traficom, 2025). Sectoral Information Sharing and Analysis Centre (ISAC) groups bring public and private experts together to exchange threat information, practise cooperation and contribute to the national situational picture (Traficom, 2025). The value lies in an established channel through which information can circulate before an incident becomes a national crisis.

Sweden illustrates another institutional configuration. Its Cybersecurity Act took effect on 15 January 2026 and implemented NIS2, while additional incident-reporting and security rules followed during 2026 (Swedish NCSC, 2026). On 1 July, national information-security and cyber functions were transferred from the Civil Defence and Resilience Agency to the National Cyber Security Centre within the National Defence Radio Establishment (FRA, 2026). The Centre's mandate includes public–private exchange and the preparation of shared threat pictures.

The Nordic examples suggest a practical answer to the public–private problem. Compliance brings reporting, but shared situational awareness requires trusted sectoral networks, protected handling of sensitive evidence, and the capacity to convert alerts into action. These arrangements should be evaluated through participation, timeliness, actionable warnings and joint incident exercises.

Poland's cybersecurity audit (August 2026)

Poland's Supreme Audit Office reviewed eight essential-service operators in energy, water and transport over January 2021–February 2026. Its August 2026 findings identified inadequate security at all eight, deficient monitoring or unaddressed alerts at six, and weaknesses in ministerial supervision (NIK, 2026). The review period includes the December 2025 energy attacks, demonstrating that formal duties do not necessarily perfectly map onto verified preparedness.

5. Cross-border dependencies

Europe's cyber exposure is shaped by dependencies that cut across operators, sectors and borders. The following cases demonstrate this clearly. KA-SAT illustrates how an attack on a common communications supplier can disrupt downstream users in several countries; the CrowdStrike outage propagated through a shared security-software update, while PHP2Shell and XZ Utils implicated software components maintained upstream of regulated entities (Council of the EU, 2022; CrowdStrike, 2024; Microsoft, 2024; PHP Foundation, 2026; CERT-EU, 2024). Supply-chain and connectivity maps should therefore identify who maintains these shared components, where alternative capacity exists, and which services cannot tolerate extended disruption.

XZ Utils software supply-chain compromise (2024)

CERT-EU (2024) documented malicious changes to XZ Utils, an open-source compression component, that could have enabled unauthorised remote access under particular configurations. The changes were detected before widespread adoption in stable software distributions. The case exposes the fragility of dependencies on software whose maintenance and security review may rest on a small number of individuals.

CrowdStrike outage (July 2024)

On 19 July 2024, a defective CrowdStrike configuration update caused Windows systems to crash and interrupted services widely, affecting an estimated 8.5 million devices (Microsoft, 2024). CrowdStrike traced the failure to problems in update validation and the release process (CrowdStrike, 2024). The incident was not malicious, which shows that even without an adversary, dependencies can interrupt services.

For industrial systems, the distinction between a compromised network and an interruption of essential services is particularly important. CERT Polska documented access to industrial installations and temporary interruption of specified processes in December 2025, even as heating continued to reach homes (CERT Polska, 2026a; 2026b). In comparison, the KA-SAT incident involved an interruption of communications supplied to downstream users (Council of the EU, 2022). Compromising an IT system does not automatically grant the ability to manipulate industrial operations.

Cross-border dependencies also have political consequences. The EU publicly attributed the KA-SAT disruption to Russia in May 2022, and a 2025 multinational advisory described Russian military-intelligence targeting of logistics and technology organisations supporting Ukraine (Council of the EU, 2022; NSA et al., 2025). These examples show how cyber operations against apparently civilian suppliers can acquire immediate security and foreign-policy significance, although this ought not to be extrapolated to a single actor behind every cyber disruption in Europe.

Between national CSIRTs and EU-wide crisis mechanisms, the Nordic–Baltic region has a further operational tier. The 2026–2029 Nordic–Baltic Cross-Border Cyber-Hub (NBCC), coordinated by Denmark with Estonia, Finland, Iceland, Latvia, Lithuania and Norway, is developing regional data sharing and access to commercial cyber-threat intelligence (CERT.LV, 2026; RIA, 2026). Estonia's Information System Authority reported that Sweden was expected to join later (RIA, 2026).

The implication is to prearrange response across national, regional and EU levels. A supplier may operate in one jurisdiction while essential services fail in several others; national CSIRTs, supervisory bodies, NBCC participants, EU-CyCLONe and private investigators may then confront overlapping requests for the same evidence or scarce technical specialists. Governments should specify incident leads, protected data-sharing procedures, evidence preservation, public messaging responsibilities and escalation paths in advance. Exercises should test simultaneous outages and competition for recovery resources, including whether essential functions can continue when rapid restoration is impossible.

6. European instruments and policy recommendations

The European Union has developed several instruments relevant to these incidents, although they perform different functions. NIS2 imposes cybersecurity risk-management and notification duties on covered entities. DORA establishes digital operational-resilience requirements for the financial sector, including oversight of critical ICT third-party providers. The Cyber Resilience Act (CRA) addresses products with digital elements. The CRA's reporting requirements for actively exploited vulnerabilities and severe product-security incidents came into effect on 11 September 2026, with specified initial and follow-up notification deadlines, while most other substantive product requirements apply from December 2027 (Regulation (EU) 2024/2847; European Commission, 2026).

At the response level, the Cyber Solidarity Act establishes provisions for national cyber hubs and an EU Cybersecurity Reserve, while the Council's June 2025 cyber crisis blueprint sets out coordination between technical and political authorities, including the European Cyber Crises Liaison Organisation Network (EU-CyCLONe) and ENISA (Regulation (EU) 2025/38; Council of the EU, 2025b). These formal frameworks should be distinguished from public attribution and foreign policy measures, which are separate political decisions taken case by case.

EU frameworks overlap with those of NATO, whose focus is collective defence. The 2024 Washington Summit Declaration agreed to establish an Integrated Cyber Defence Centre (NATO, 2024). The 2023 Vilnius Summit Communiqué states that a single malicious cyber activity, or the cumulative effects of several, could reach the level of an armed attack and lead the North Atlantic Council to invoke Article 5 on a case-by-case basis (NATO, 2023, para. 66). Neither document, however, sets an automatic threshold.

The following recommendations are directed to member-state governments and supervisors, national CSIRTs, European institutions and essential-service operators. They build on the documented incidents and seek measurable resilience, coordinated response and credible consequences:

- **Map essential functions and their shared dependencies.** Member-state supervisory authorities should require covered operators to identify software maintainers, update channels, cloud and remote-access providers, satellite links and cross-border supply nodes on which minimum service depends. ENISA and sectoral bodies can facilitate common mapping methods. The KA-SAT, PHP2Shell and XZ Utils cases show why an inventory confined to an operator's own equipment is inadequate.
- **Keep essential services running through prolonged disruption.** Operators, supported by regulators and emergency planners, should set and exercise minimum-service levels, independent communications, manual workarounds, isolation procedures and reserves of personnel and supplies. Restoration targets matter, but the Polish energy attacks demonstrate the separate value of continuing heat and electricity provision while systems are compromised. Cross-sector exercises must test simultaneous demands on scarce recovery resources.
- **Build usable public–private information exchange.** National CSIRTs and supervisory authorities should combine NIS2 notifications with protected channels for voluntary intelligence, sectoral ISAC participation, and arrangements for preserving technical evidence. The Commission and ENISA should advance compatible reporting interfaces while retaining the information needed for incident response. Finland and Sweden illustrate institutional approaches, while the Polish audit shows the consequences when monitoring and supervision remain weak.

- **Prearrange regional and cross-border incident response.** Member states should exercise procedures linking national CSIRTs, the Nordic–Baltic Cross-Border Cyber-Hub, EU-CyCLONe and relevant EU institutions, as well as NATO where collective-defence issues arise. Critical suppliers and private responders must participate. Exercises should test shared situational awareness, requests for assistance, evidence preservation, public communication and competing demands on the same technical specialists, as illustrated by KA-SAT and the CrowdStrike outage.
- **Use attribution and consequences selectively and transparently.** The Council and member states should distinguish technical findings from political attribution and legal responsibility, and evaluate sanctions and law-enforcement actions through enforceable costs and observable disruption. Offensive cyber operations should remain an option when lawful, intelligence-led, proportionate to the expected objective and assessed for third-party and escalation effects. The KA-SAT attribution and Operation Eastwood illustrate different instruments, with different measures of success.

7. Conclusion

Three findings emerge. First, the European record documents effective defence, partial disruption and sometimes rapid recovery, but offers limited direct evidence that particular adversaries were deterred from attempting attacks. Resilience should therefore be judged primarily by continued service and the containment of harm. Second, the exposure of critical infrastructure extends upstream into shared software, connectivity and suppliers, where individual operators and entity-based regulation provide only partial coverage.

Third, effective response depends on the quality of connections between private operators, national authorities, regional partners and EU institutions. Finland's exchange networks, Sweden's institutional consolidation and the developing Nordic–Baltic cyber hub provide exemplary concrete arrangements. The immediate European priorities are sustained continuity under attack, visibility of cross-border dependencies and prearranged cooperation. Attribution, sanctions, criminal justice and selected offensive cyber operations retain important roles when their objectives, authorities and likely effects are specified in advance.

References

Amazon (2026) 'Amazon Threat Intelligence identifies PHP2Shell exploitation prior to public disclosure in MadPot', AWS Security Blog, 21 October. Available at: https://aws.amazon.com/blogs/security/amazon-threat-intelligence-identifies-php2shell-exploitation-prior-to-public-disclosure-in-madpot/.

Bendiek, A. and Bund, J. (2024) 'Hardening Norms and Networks: Europe's Cyber Defence Posture', Intereconomics, 59(4), pp. 198–203.

Bendiek, A. and Hemmelskamp, J. (2025) EU Cyber Posture: Why Cyber Deterrence does not work (yet). SWP Working Paper No. 07, August 2025. Berlin: Stiftung Wissenschaft und Politik. Available at: https://www.swp-berlin.org/publications/products/arbeitspapiere/Bendiek_Hemmelskamp_EU_Cyber_Posture_SWP_WP_25_07.pdf.

CERT Polska (2026a) 'Energy Sector Incident Report – 29 December 2025', 30 January. Available at: https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/.

CERT Polska (2026b) 'Follow-Up Report of the December 2025 Energy Sector Incident', 8 August. Available at: https://cert.pl/en/posts/2026/08/incident-follow-up-report-energy-sector-2025/.

CERT-EU (2024) 'Critical Vulnerability in XZ Utils', Security Advisory 2024-032, updated 2 April. Available at: https://www.cert.europa.eu/publications/security-advisories/2024-032/.

CERT.LV (2026) 'International projects: Nordic-Baltic Cross-Border Cyber-Hub (NBCC)'. Available at: https://cert.lv/en/about-us/international-projects.

CISA (2026) Known Exploited Vulnerabilities Catalog, entries for CVE-2026-109618 and CVE-2026-109619 added 26 October 2026. Washington, DC: Cybersecurity and Infrastructure Security Agency. Available at: https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

CISA, NSA, FBI and partner agencies (2024) PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. Joint Cybersecurity Advisory AA24-038A, 7 February 2024. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers. Official Journal of the European Union, L, 2024/2690, 18 October 2024.

Consolidated version of the Treaty on the Functioning of the European Union. Official Journal of the European Union, C 202, 7 June 2016, p. 47.

Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Official Journal of the European Union, L 129 I, 17 May 2019, p. 13. Consolidated version of 13 July 2026, CELEX 02019D0797-20260713. Available at: https://eur-lex.europa.eu/eli/dec/2019/797/2026-07-13/eng.

Council of the EU (2022) 'Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union', 10 May. Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/.

Council of the EU (2023) Revised Implementing Guidelines of the Cyber Diplomacy Toolbox. Council document 10289/23, 8 June 2023. Available at: https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf.

Council of the EU (2025a) 'Cyber-attacks: three individuals added to EU sanctions list for malicious cyber activities against Estonia', 27 January. Available at: https://www.consilium.europa.eu/en/press/press-releases/2025/01/27/cyber-attacks-three-individuals-added-to-eu-sanctions-list-for-malicious-cyber-activities-against-estonia/.

Council of the EU (2025b) 'EU adopts blueprint to better manage European cyber crises and incidents', 6 June. Available at: https://www.consilium.europa.eu/en/press/press-releases/2025/06/06/eu-adopts-blueprint-to-better-manage-european-cyber-crises-and-incidents/.

Council of the EU (2026a) 'Cyber-attacks against the EU and its member states: Council sanctions three entities and two individuals', 16 March. Available at: https://www.consilium.europa.eu/en/press/press-releases/2026/03/16/cyber-attacks-against-the-eu-and-its-member-states-council-sanctions-three-entities-and-two-individuals/.

Council of the EU (2026b) 'Russian cyber-attacks and destabilising activities: Council sanctions nine individuals and four entities', 13 July. Available at: https://www.consilium.europa.eu/en/press/press-releases/2026/07/13/russian-cyber-attacks-and-destabilising-activities-council-sanctions-nine-individuals-and-four-entities/.

CrowdStrike (2024) ‘Channel File 291 Incident: Root Cause Analysis is Available’, 6 August. Available at: https://www.crowdstrike.com/en-us/blog/channel-file-291-rca-available/.

CrowdStrike (2026) ‘Obstacles to Weaponizing PHP2Shell Likely Constrain Immediate Widespread Exploitation’, 23 October. Available at: https://www.crowdstrike.com/en-us/blog/obstacles-to-weaponizing-php2shell-likely-constrain-exploitation/.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union, L 194, 19 July 2016, pp. 1–30.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union, L 333, 27 December 2022, pp. 80–152.

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union, L 333, 27 December 2022, pp. 164–198.

Egloff, F.J. (2020) ‘Public attribution of cyber intrusions’, Journal of Cybersecurity, 6(1), tyaa012.

ENISA (2024) 2024 Report on the State of the Cybersecurity in the Union. Athens: European Union Agency for Cybersecurity, December 2024. Available at: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union.

ENISA (2025) NIS Investments 2025. Athens: European Union Agency for Cybersecurity, December 2025. Available at: https://www.enisa.europa.eu/publications/nis-investments-2025.

ENISA (2026a) ENISA NIS360: Latest insights in the cybersecurity maturity and criticality of NIS sectors of high criticality. Athens: European Union Agency for Cybersecurity, May 2026. Available at: https://www.enisa.europa.eu/sites/default/files/2026-05/ENISA%20NIS360%202026.pdf.

ENISA (2026b) ENISA Threat Landscape 2026. Athens: European Union Agency for Cybersecurity, September 2026. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2026.

European Commission (2024) The Commission calls on 23 Member States to fully transpose the NIS2 Directive. News item, 28 November 2024. Available at: https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive.

European Commission (2025) Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus). COM(2025) 837 final, 2025/0360(COD), 19 November 2025.

European Commission (2026) ‘Cyber Resilience Act – Reporting obligations’, updated 11 September. Available at: https://digital-strategy.ec.europa.eu/en/policies/cra-reporting.

Eurojust (2025) ‘Hacktivist group responsible for cyberattacks on critical infrastructure in Europe taken down’. Press release, 16 July 2025. Available at: https://www.eurojust.europa.eu/news/hacktivist-group-responsible-cyberattacks-critical-infrastructure-europe-taken-down.

Europol (2025) ‘Global operation targets NoName057(16) pro-Russian cybercrime network’, 16 July. Available at: https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network.

FRA (2026) ‘Nationellt cybersäkerhetscenter, NCSC’. Försvarets radioanstalt. Available at: https://www.fra.se/cyberforsvar/ncsc.4.766e440918f572e733597.html.

Gauch, K., Georg Schaffner, L., Behnam, E. and Prinz, E. (2026) ‘European cybersecurity disclosure practices: a textual analysis’, International Journal of Disclosure and Governance, 23(3), pp. 871–885.

Government of Poland (2026) ‘Poland Stops Cyberattacks on Energy Infrastructure’, Chancellery of the Prime Minister, 15 January. Available at: https://www.gov.pl/web/primeminister/poland-stops-cyberattacks-on-energy-infrastructure/.

Microsoft (2024) ‘Helping our customers through the CrowdStrike outage’, Official Microsoft Blog, 20 July. Available at: https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/.

NATO (2023) Vilnius Summit Communiqué, 11 July 2023, para. 66. Available at: https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

NATO (2024) Washington Summit Declaration, 10 July 2024. Available at: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/washington-summit-declaration.

NATO (2026) Guidance for enhancing public-private cooperation for resilience. Official text, 16 July 2026. Available at: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/07/16/guidance-for-enhancing-public-private-cooperation-for-resilience.

NSA, FBI, NCSC and partner agencies (2025) Russian GRU Targeting Western Logistics Entities and Technology Companies. Joint Cybersecurity Advisory, Australian Cyber Security Centre edition, published 22 May 2025. Available at: https://www.cyber.gov.au/advisory/russian-gru-targeting-western-logistics-entities-and-technology-companies.

NIK (2026) 'Transport, energy, and drinking water supplies are inadequately protected against cyberattacks', Najwyższa Izba Kontroli (Supreme Audit Office), 27 August. Available at: https://www.nik.gov.pl/en/news/transport-energy-and-drinking-water-supplies-are-inadequately-protected-against-cyberattacks.html.

NIS Cooperation Group (2025) Annual report NIS Directive incidents 2024. CG Publication, August 2025. Available at: https://ec.europa.eu/newsroom/repository/document/2025-31/Annual_Report_NISD_Security_Incidents_2024_ILI8Yt8at5UKGOymYgsc0rxZ-rpQ_118680.pdf.

Nye, J.S. Jr. (2017) 'Deterrence and dissuasion in cyberspace', International Security, 41(3), pp. 44–71.

Palo Alto Networks Unit 42 (2026) 'Threat Brief: Critical Vulnerabilities in PHP: CVE-2026-109618, CVE-2026-109619', updated 29 October. Available at: https://unit42.paloaltonetworks.com/cve-2026-109618-cve-2026-109619/.

PHP Foundation (2026) 'Today's PHP Security Release, and How We're Strengthening PHP Security', 21 October. Available at: https://thephp.foundation/blog/2026/10/21/todays-php-security-release-and-how-were-strengthening-php-security/.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 4 May 2016, pp. 1–88.

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA). Official Journal of the European Union, L 333, 27 December 2022, pp. 1–79.

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). Official Journal of the European Union, L, 2024/2847, 20 November 2024.

Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act). Official Journal of the European Union, L, 2025/38, 15 January 2025.

RIA (2026) 'What to expect in cyberspace in 2026', Estonian Information System Authority, updated 11 February. Available at: https://ria.ee/en/what-expect-cyberspace-2026.

Schmitz-Berndt, S. (2023) 'Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive', Journal of Cybersecurity, 9(1), tyad009.

Serini, F. (2024) 'Collective cyber situational awareness in EU. A political project of difficult legal realisation?', Computer Law & Security Review, 55, 106055.

Swedish NCSC (2026) 'Tidsplan för införandet av cybersäkerhetslagen i Sverige', National Cyber Security Centre. Available at: https://www.ncsc.se/sv/radgivning-och-stod/cybersakerhetslagen-nis2/tidsplan-for-inforandet-av-cybersakerhetslagen-i-sverige/.

Traficom (2025) 'Incident notification under the NIS 2 Directive', National Cyber Security Centre Finland, updated 8 April. Available at: https://www.kyberturvallisuuskeskus.fi/en/incident-notification-under-nis-2-directive.

Traficom (n.d.) 'ISAC information sharing groups', National Cyber Security Centre Finland. Available at: https://kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

Web-Performance (2025) 'NoName057(16) returns after Police raid', 23 July. Available at: https://web-performance.ch/security/noname05716-returns-after-police-raid/ .

GLOBSEC
IDEAS SHAPING THE WORLD

Vajnorská 100/B
831 04 Bratislava
Slovak Republic

+421 2 3213 7800
info@globsec.org
www.globsec.org