Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

The AI Act's Blind Side? Dependency Risk, Hybrid Warfare and the Fragmented Governance of Critical AI Infrastructure

Robert Pakla

rpakla@gmail.com

Research Article

Keywords: AI Act, DORA, NIS2 Directive, Cyber Resilience Act, CER Directive, hybrid warfare, ICT concentration risk, supply-chain security, technofascism, operational sovereignty

Posted Date: November 4th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11236039/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

The AI Act's Blind Side? Dependency Risk, Hybrid Warfare and the Fragmented Governance of Critical AI Infrastructure

Abstract

Regulation (EU) 2024/1689 (the AI Act) is the most comprehensive attempt so far to subject artificial intelligence to a horizontal legal regime. Its conceptual centre of gravity is the individual AI system and the risks it poses to health, safety and fundamental rights. This article argues that in an environment of hybrid conflict the decisive security risk increasingly lies outside the model: in cloud and identity infrastructure, software supply chains, privileged vendor access, telecommunications and data-integration platforms, and in the small number of providers capable of operating them at scale. On the basis of the European Union's July 2026 attribution of sabotage operations against Polish combined heat and power plants to the 16th Centre of the Russian FSB, CERT Polska's analyses of the December 2025 attacks on the energy sector and of the UNC1151 phishing campaign, and the 2026 compromises of healthcare and invoicing software providers in Poland, the article reconstructs the category of dependency risk and contrasts it with the model-centred concept of risk adopted in the AI Act, including its Article 9(3), which confines risk management to risks that can be addressed through the design of the system. It proposes a structural definition of technofascism as a failure mode in which concentrated informational power, automated decision capacity and infrastructural dependence become fused with coercive political power. Its principal claim is that the limitation lies not in the absence of cybersecurity regulation within the AI Act, but in the fragmentation of dependency governance across the AI Act, the Digital Operational Resilience Act, the NIS2 Directive, the Cyber Resilience Act, the Critical Entities Resilience Directive and adjacent Union legislation. While these instruments regulate different layers of the same technological architecture, they do not establish a common method for identifying sector-wide concentration, transitive supplier dependencies and the consequences of losing trust in a strategically positioned provider. The article concludes with control domains for the operational resilience of critical AI deployments, proposes a cross-regulatory dependency map and argues that the central question of European AI governance is shifting from the safety of systems to the control of control planes.

Keywords: AI Act; DORA; NIS2 Directive; Cyber Resilience Act; CER Directive; hybrid warfare; ICT concentration risk; supply-chain security; technofascism; operational sovereignty

1. Introduction

The AI Act[1] is the most ambitious attempt so far to place artificial intelligence within a comprehensive legal architecture. Its method is risk-based: it asks whether an AI system threatens health, safety or fundamental rights, whether a given practice should be prohibited, whether a high-risk system is sufficiently accurate, robust and cybersecure, and whether a

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence [...] (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024), as amended by Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) (OJ L, 2026/1744, 24.7.2026), hereinafter: AI Act. Regulation (EU) 2026/1744 entered into force on 27 July 2026.

general-purpose model may generate systemic risk. These questions remain indispensable. In the present security environment, however, they no longer exhaust the problem they were meant to address.

The strategic risk now emerging in Europe resides not only inside the algorithm but in the infrastructure that surrounds it: cloud environments, identity providers, data-integration platforms, telecommunications networks, software supply chains, privileged vendor access, third-party libraries, managed services and the comparatively small group of corporations able to operate these layers at scale. Under conditions of hybrid conflict it is precisely these layers that are targeted. In July 2026 the European Union publicly identified the 16th Centre of the Russian Federal Security Service (FSB) as controlling several cyber threat groups, including Turla, and stated that it had recently carried out disruptive sabotage operations against Polish critical infrastructure, including combined heat and power plants.[2] In the same period Poland faced an intensive phishing campaign directed against politically and strategically exposed persons[3] and a series of breaches at software providers serving thousands of medical practices, one of which potentially concerns the data of 18.8 million people.[4]

Against this background the regulatory question changes. It concerns not only what an AI system can do, but also who controls the technological infrastructure on which the system depends, who is able to compromise that infrastructure, how many institutions rely on the same supplier, and what remains operational when the supplier, its software supply chain, its privileged identities or its control plane are compromised. The thesis of this article is that this question exposes a limit not of the AI Act alone but of the way in which Union law distributes dependency risk across several regimes. The AI Act does not operationalise dependency risk as a distinct governance category, while the regulatory logic developed in the Digital Operational Resilience Act (DORA)[5] and in the NIS2 Directive[6], complemented by the Cyber Resilience

[2] Council of the European Union, 'Cyber / Russia: Statement by the High Representative on behalf of the European Union denouncing Russia's malicious cyber ecosystem targeting the EU, its member states and international partners' (press release, 13 July 2026) <https://www.consilium.europa.eu/en/press/press-releases/2026/07/13/cyber-russia-statement-by-the-high-representative-on-behalf-of-the-european-union-denouncing-russia-s-malicious-cyber-ecosystem-targeting-the-eu-its-member-states-and-international-partners/> accessed 1 October 2026.

[3] CERT Polska, 'UNC1151/Ghostwriter phishing campaign targeting Gmail accounts' (12 June 2026) <https://cert.pl/en/posts/2026/06/UNC1151-gmail-campaign/> accessed 1 October 2026.

[4] The incidents are discussed, with sources, in Section 4.

[5] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector [...] (OJ L 333, 27.12.2022, p. 1), hereinafter: DORA.

[6] 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

Act (CRA)[7] and the Critical Entities Resilience Directive (CER Directive),[8] addresses different layers of the same architecture without supplying a common method for mapping the dependencies between them.

The analysis is doctrinal and problem-oriented. The concept of risk adopted in the AI Act is reconstructed from its text as amended by Regulation (EU) 2026/1744, confronted with publicly documented incidents and official attributions, and compared with the third-party and supply-chain provisions of DORA and NIS2, including the Polish transposition of the latter, as well as with adjacent Union legislation. Incidents serve to illustrate mechanisms; no attribution is asserted beyond what the cited public sources state. The legal and factual position is that of 1 October 2026. Section 2 examines the object of protection in the AI Act, Section 3 develops technofascism as an analytical category, Section 4 analyses the hybrid threat environment on the basis of Polish incidents from 2025 and 2026, and Section 5 turns to the concentration of digital power, including the case of Palantir. Section 6 places DORA and NIS2 within the wider EU resilience architecture, including the CRA and the CER Directive, Section 7 translates it into control domains for critical AI deployments, and Section 8 contains the conclusions.

2. The object of protection in the AI Act: systems rather than dependencies

The AI Act is commonly described as risk-based legislation. The description is accurate but incomplete, because the decisive question is which risks the Regulation is designed to conceptualise. Article 9 requires a risk-management system for high-risk AI systems, understood as a continuous and iterative process run throughout the lifecycle of the system, whose first step is the identification and analysis of the known and reasonably foreseeable risks that the system can pose to health, safety or fundamental rights when used in accordance with its intended purpose.[9] Article 9(3) then narrows the exercise in a manner that is decisive for the present argument: the risks concerned are only those which may be reasonably mitigated or eliminated through the development or design of the high-risk AI system, or through the

Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80), hereinafter: NIS2.

[7] 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 and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024), hereinafter: CRA.

[8] 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 (OJ L 333, 27.12.2022, p. 164), hereinafter: CER Directive.

[9] AI Act, art 9(1) and (2)(a); the text is available through the European Commission's AI Act Service Desk <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-9> accessed 1 October 2026.

provision of adequate technical information.[10] Risks whose source lies outside the system and which its design cannot meaningfully reduce, such as the simultaneous dependence of an entire sector on a single cloud control plane, are therefore structurally marginal to the provider's risk-management obligation.

Article 15 adds requirements of accuracy, robustness and cybersecurity. Its fourth paragraph requires high-risk systems to be as resilient as possible regarding errors, faults or inconsistencies that may occur within the system or the environment in which it operates, and contemplates technical redundancy solutions, including backup or fail-safe plans. Its fifth paragraph requires high-risk systems to be resilient against attempts by unauthorised third parties to alter their use, outputs or performance by exploiting system vulnerabilities, a formula broad enough to reach vulnerabilities outside the model itself, and adds that technical solutions addressing AI-specific vulnerabilities are to include, where appropriate, measures against the manipulation of the training data set (data poisoning) or of pre-trained components (model poisoning), against inputs designed to cause the model to make a mistake (adversarial examples or model evasion), and against confidentiality attacks and model flaws.[11] For general-purpose AI models with systemic risk the Regulation goes further and requires providers to ensure an adequate level of cybersecurity protection for the model and for its physical infrastructure.[12] The concept of systemic risk itself, however, is defined by reference to the high-impact capabilities of such models and to negative effects that can be propagated at scale across the value chain,[13] and not by reference to the concentration of the infrastructure on which deployers depend.

Nor is the AI Act indifferent to dependencies along the AI value chain. Article 25(4), as amended in 2026, requires the provider of a high-risk AI system and the third party that supplies an AI system, AI model, tools, services, components or processes used or integrated in that system to specify, by written agreement, the information, capabilities, technical access and other assistance necessary for the provider to comply with the Regulation, and a breach of that

[10] AI Act, art 9(3). Recital 65 adds that the process should also cover risks arising from the interaction between the AI system and the environment within which it operates; the reference, however, remains anchored in the risks of the system itself.

[11] AI Act, art 15(1), (4) and (5). Recital 76 states that cyberattacks against AI systems may also exploit vulnerabilities in the system's digital assets or in the underlying ICT infrastructure, and that providers should take suitable security controls, taking that infrastructure into account as appropriate.

[12] AI Act, art 55(1)(d). According to recital 115, that protection may be facilitated by securing model weights, algorithms, servers and data sets, including through operational security measures and cyber and physical access controls.

[13] AI Act, art 3(65).

obligation is now expressly subject to administrative fines.[14] This is a meaningful supply-chain mechanism. It does not, however, amount to a regime for measuring concentration, substitutability or sector-wide dependence on common infrastructure, because it governs the bilateral relationship between a provider and its supplier rather than the aggregate exposure of many deployers to the same supplier. The post-2026 architecture also makes the division of regulatory labour explicit. Under the new Article 42(3), high-risk AI systems falling within the scope of the CRA are deemed to comply with the cybersecurity requirements of Article 15 where the conditions laid down in Article 12(1) of the CRA are fulfilled.[15] The legislature therefore treats the cybersecurity of AI as part of a composite regulatory architecture rather than as a self-contained function of the AI Act.

These provisions are significant, and the criticism developed here does not concern their quality. It concerns their architecture. The limitation identified in this article is not that the AI Act disregards cybersecurity or the environment of the AI system. It is that the Regulation does not operationalise supplier concentration, substitutability, infrastructure dependency and loss-of-trust scenarios as autonomous risk variables comparable to those developed in DORA and the wider EU resilience framework. The obligations attach to the AI system or model as a product placed on the market or put into service, and the attack surface they describe is centred on the system, its model and its data, with the underlying infrastructure taken into account as part of the system's own security. The dependency graph in which the system operates appears through the environment clause of Article 15(4), recital 76 and the contractual mechanism of Article 25(4), but not as an object of measurement in its own right. A contemporary AI deployment, however, is rarely an autonomous artefact; it is a node in a graph of dependencies. A bank may operate an AI-based fraud-detection engine while authentication relies on one identity provider, workloads run with one hyperscaler, telemetry is collected by another vendor, data enrichment depends on several external interfaces, inference is supplied by an external model provider, development draws on open-source packages and deployment is managed on an orchestration platform operated by a third party. A public authority may own the legal decision without owning the technical stack through which that decision is produced.

[14] Article 25(4), first subparagraph, AI Act as replaced by art 1, point 12(b), of Regulation (EU) 2026/1744 (n 1), and art 99(4)(da) AI Act as inserted by art 1, point 38(b), of that Regulation; the official text is reproduced at <https://artificialintelligenceact.eu/ai-act-explorer/digital-omnibus/> accessed 1 October 2026.

[15] Article 42(3) AI Act as added by art 1, point 18, of Regulation (EU) 2026/1744 (n 1); CRA (n 7), art 12(1) and recital 51, according to which the presumption extends to the requirements of Article 15 in so far as they are covered by the EU declaration of conformity issued under the CRA.

It is therefore possible for every identifiable AI component to satisfy its immediate regulatory requirements while the aggregate architecture remains systemically fragile. An attacker has no need to manipulate a model if the administrator of that model can be compromised, nor to poison a decision engine if its upstream data can be altered. An AI system need not be hacked at all where the identity provider authenticating its users is under hostile control, and encryption offers limited comfort to an organisation whose adversary holds legitimate privileged credentials. Redundancy within a single organisation becomes largely illusory where its nominally independent services ultimately depend on the same cloud, telecommunications, identity or software-supply-chain provider. This is a conception of systemic risk different from the one traditionally associated with model behaviour, and it may be described as dependency risk.

The temporal dimension sharpens the contrast. Regulation (EU) 2026/1744 deferred the application of the requirements for high-risk AI systems, which now apply from 2 December 2027 to systems listed in Annex III and from 2 August 2028 to systems covered by the Union harmonisation legislation listed in Annex I.[16] At the date of writing, therefore, Articles 9 and 15 do not yet bind providers of stand-alone high-risk systems, whereas DORA has applied since 17 January 2025[17] and the deadline for the transposition of NIS2 expired in October 2024.[18] Operational-resilience law is already in force in precisely the areas in which the AI Act's own risk regime has been postponed.

The limit becomes most visible in Article 2(3), under which the Regulation does not apply to AI systems placed on the market, put into service or used, with or without modification, exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.[19] The allocation of competence reflects Article 4(2) TEU and is legally understandable. It has nevertheless been criticised as difficult to reconcile with the case law of the Court of Justice, which confines the national security exception to purely governmental activity, and as difficult to apply given the fluid boundary between national and public security; where the same system also serves law enforcement or public security purposes,

[16] Article 113, third paragraph, point (c), AI Act as replaced by Regulation (EU) 2026/1744 (n 1). For the consolidated calendar see Future of Privacy Forum, 'EU AI Act Implementation Timeline (updated following the AI Omnibus)' (July 2026) <https://fpf.org/wp-content/uploads/2026/07/FPF-EU-AI-Act-Timeline-2026-R2.pdf> accessed 1 October 2026.

[17] DORA, art 64.

[18] NIS2, art 41(1).

[19] AI Act, art 2(3); see the text published by the AI Act Service Desk <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-2> accessed 1 October 2026.

the Regulation applies.[20] Operationally, hybrid conflict ignores this taxonomy. The hospital whose records are exfiltrated today may treat a military officer tomorrow; the telecommunications operator serving consumers also carries government traffic; the cloud provider hosting a retailer may host a defence subcontractor in the neighbouring tenant; and the identity system used for routine administration may authenticate persons with access to classified information. Hybrid operations exploit the relationships between systems, whereas regulation divides those systems into sectors and purposes, and the resulting mismatch is becoming increasingly consequential.

3. Technofascism as an analytical category

'Technofascism' is analytically hazardous precisely because it is rhetorically powerful. Used loosely, it degenerates into an accusation that can be directed at any government, corporation, surveillance technology or political position, and it then loses explanatory value. The recent literature nevertheless employs the term to examine convergences between artificial intelligence, platform power, surveillance, behavioural manipulation, concentrated technological resources and authoritarian politics. Coeckelbergh argues that features of contemporary digital technologies, of their governance and of their political context mirror features of historical fascism, and calls for systemic changes in both the development of technologies and the governance of technology and society.[21] The adjacent literature on digital authoritarianism acknowledges, in turn, that this term and related ones, such as networked authoritarianism, digital repression and techno-authoritarianism, are frequently used without clear definition, which undermines comparative research.[22]

For the purposes of legal analysis, technofascism should not be treated as a synonym for Big Tech, for any particular company, for artificial intelligence, for algorithmic administration or even for digital authoritarianism. A more defensible definition is structural. Technofascism denotes a potential political-technological failure mode in which concentrated digital infrastructure, pervasive data aggregation and automated decision capability become integrated

---

[20] P Vogiatzoglou, 'The AI Act National Security Exception: Room for Manoeuvres?' (*Verfassungsblog*, 9 December 2024) <https://verfassungsblog.de/the-ai-act-national-security-exception/> accessed 1 October 2026, DOI 10.59704/292082becc7cc8e6, discussing in particular the judgment in *La Quadrature du Net* and recital 24 of the AI Act.

[21] M Coeckelbergh, 'Technofascism: AI, Big Tech, and the New Authoritarianism' *AI & Society* (published online 25 January 2026) <https://doi.org/10.1007/s00146-026-02862-9> accessed 1 October 2026.

[22] T Roberts and M Oosterom, 'Digital Authoritarianism: A Systematic Literature Review' *Information Technology for Development* (2024), abstract available at <https://mediawell.ssrc.org/?p=513012> accessed 1 October 2026.

with coercive political power to such an extent that meaningful institutional contestability, individual autonomy and practical alternatives to the dominant technological order disappear. The category is normative and structural; it is not an allegation concerning the political character or intentions of any company discussed in this article.

The definition has five elements. The first is the concentration of informational power, which consists not in holding large quantities of data but in the ability to link identity, location, finance, communications, health, employment, behavioural and relational data into a single operational representation of a person or of a population. Decision capability forms the second element: data cease merely to describe reality and begin to determine access, prioritisation, investigation, intervention or exclusion. Infrastructural dependence is the third, since a state or a society may remain formally free to reject a given technology provider while becoming operationally incapable of doing so, because migration has become economically, institutionally or technically prohibitive. The fourth element combines opacity with asymmetry of power, in that those subject to the system have neither effective knowledge of its operation nor practical means of contesting its outputs. The fifth, and decisive, element is the link between technological capacity and political coercion.

This structural account corresponds to the theory of weaponised interdependence developed by Farrell and Newman, who show that highly asymmetric networks allow actors with effective jurisdiction over central nodes to gather strategically valuable information (the panopticon effect) and to deny network access to adversaries (the chokepoint effect).[23] Their analysis concerns states with jurisdiction over global financial and informational networks. It can be extended to digital infrastructure: whoever controls, or succeeds in compromising, a central node of identity, cloud or data integration acquires both effects without having to control the network as a whole.

A data platform used by a democratic institution that is subject to judicial review, effective access control, pluralistic oversight and enforceable legal limits does not become fascist by virtue of its technological sophistication. The same architecture becomes extraordinarily consequential, however, once it is embedded in a political order prepared to use it for systematic repression. The risk therefore lies not necessarily in the intentions of the present operator but in the transferability of technological power across governments, administrators and regimes. A database persists after a change of government and an ontology outlives elections; an identity

[23] H Farrell and AL Newman, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion' (2019) 44(1) *International Security* 42-79.

graph assembled for fraud prevention can technically be repurposed for intelligence, and infrastructure built for legitimate purposes can later serve coercion. For that reason the democratic governance of advanced technology cannot rest on the benevolence of whoever operates it at a given moment.

External compromise is the other side of the same structure. An architecture that concentrates informational and decision power is attractive both to a domestic actor tempted by coercion and to a foreign service seeking leverage, and the safeguards that protect against the former, such as separation, least privilege, auditability and the ability to revoke trust, largely coincide with those that protect against the latter. This is the point at which the concept of technofascism meets the practice of hybrid warfare.

4. The hybrid threat environment: evidence from Poland

The incidents discussed in this and the following section are not presented as infringements of the AI Act, nor necessarily as incidents involving AI. They serve as empirical observations of compromise mechanisms, namely identity capture, supplier compromise, software-supply-chain poisoning, abuse of privileged access and infrastructure concentration, which remain relevant whenever AI systems are deployed on top of the same technological layers.

Cybersecurity has traditionally been conceptualised through confidentiality, integrity and availability. Hybrid conflict adds a fourth dimension, namely strategic exploitation, understood as the use of access, data and dependence for political, intelligence or coercive purposes. On 13 July 2026, in a statement issued by the High Representative on behalf of the Union, the EU and its Member States denounced Russia's use of a cyber ecosystem comprising intelligence services, cybercriminal groups, hacktivists and private companies, identified the FSB's 16th Centre as controlling a variety of threat groups including Turla, and stated that these activities had included the infiltration of governmental networks and the sabotage of critical infrastructure, among them disruptive sabotage operations in Poland against combined heat and power plants.[24] On the same day the Council imposed restrictive measures on nine individuals and four entities, including GRU officers, cybercriminals, self-proclaimed hacktivists and private companies.[25]

The technical record is consistent with this attribution. According to CERT Polska, on 29 December 2025 coordinated destructive attacks targeted at least 30 wind and photovoltaic

[24] Council statement (n 2).

[25] Ibid; CERT-EU, 'Cyber Brief 26-08: July 2026' <https://cert.europa.eu/publications/threat-intelligence/cb26-08> accessed 1 October 2026.

farms, a manufacturing company and a large combined heat and power plant supplying heat to almost half a million customers. The attacks on renewable installations severed communication between the facilities and the distribution system operators without affecting ongoing generation, while the wiper deployed at the large plant, preceded by long-term infiltration, theft of information and the acquisition of privileged accounts, was blocked by endpoint detection and response software.[26] CERT Polska found that the infrastructure used overlapped substantially with that of the activity cluster publicly tracked as Static Tundra, Berserk Bear, Ghost Blizzard and Dragonfly, and noted that this was the first publicly described destructive activity attributed to that cluster.[27] Private-sector reporting was not uniform, as other analysts linked the operation to Sandworm.[28] The divergence shows why attribution must remain evidence-based, and also why a resilience-oriented legal response cannot be made conditional upon it.

The follow-up report published on 8 August 2026 describes an additional attack carried out on the same day against a smaller plant supplying heat to about 50,000 residents. The attacker switched controllers into stop mode, halting a steam turbine and a water treatment station for technical purposes and thereby interrupting cogeneration; the operator, which was conducting maintenance work at the time, initially attributed the stoppage to an error by a subcontractor's engineers and reported the event for information only.[29] The path of the attack is instructive. From a wind farm whose internet-facing VPN and firewall device allowed logins without multi-factor authentication, the attacker reached a cellular router connected to a private access point name (APN) operated by the distribution system operator, scanned that network and found at the plant a controller whose administrative web panel was reachable through the APN and protected by default credentials.[30] CERT Polska regards this as the first observed real-world

[26] CERT Polska, 'Raport z incydentu w sektorze energii z 29 grudnia 2025 roku' [Report on the energy sector incident of 29 December 2025] (30 January 2026) <https://cert.pl/posts/2026/01/raport-incydent-sektor-energii-2025/> accessed 1 October 2026.

[27] Ibid.

[28] ITwiz, 'Za grudniowym atakiem na polską energetykę stoi rosyjska grupa Sandworm' <https://itwiz.pl/?p=69814> accessed 1 October 2026 (reporting the analysis of ESET); SecurityWeek, 'Novel Private APN Pivot Let Hackers Sabotage Second Polish Energy Facility' <https://www.securityweek.com/novel-private-apn-pivot-let-hackers-sabotage-second-polish-energy-facility/amp/> accessed 1 October 2026.

[29] CERT Polska, 'Follow-Up Report of the December 2025 Energy Sector Incident' (8 August 2026) <https://cert.pl/en/posts/2026/08/incident-follow-up-report-energy-sector-2025/> accessed 1 October 2026; full text: CERT Polska, *Uzupełnienie raportu z incydentu w sektorze energii 29 grudnia 2025* [Supplement to the report on the energy sector incident of 29 December 2025] <https://cert.pl/uploads/docs/CERT_Polska_Uzupelnienie_Raportu_Incydent_Sektor_Energii_2025.pdf> accessed 1 October 2026, 4-5 and 11.

[30] CERT Polska, Supplement (n 29) 7-9 and 13.

use of a private APN as an attack vector, made possible, among other factors, by a configuration that allowed arbitrary devices within the APN to communicate with one another, and reports that surveys of entities using such solutions showed this configuration to be common in Poland at the time.[31] The vulnerability was not a defective algorithm. It lay in architecture, configuration, connectivity and operational practice, distributed across the wind farm operator, its integrator, the distribution system operator and the plant. None of these incidents depended on the presence of an AI system. Their relevance is architectural: they demonstrate attack paths that a critical AI deployment would inherit from the infrastructure in which it operates. The link with the AI Act is nonetheless direct, since Annex III, point 2, classifies as high-risk the AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity.[32] A high-risk system of that kind, once deployed in a heat and power plant, would run on precisely the connectivity exploited in December 2025.

The espionage dimension is equally visible. CERT Polska describes the UNC1151/Ghostwriter group as one of the most active advanced persistent threat actors it monitors. Since March 2026 the group has conducted high-intensity phishing campaigns against Gmail users that enable the theft of two-factor authentication codes; once an account has been compromised, the attackers search it for contact lists used to identify further targets, for sensitive documents and for linked accounts. The targets include persons active in political and public life, researchers, journalists, employees of public administration and law enforcement and persons connected to them, as well as particular professional groups such as translators and court experts.[33] Mandiant assessed with high confidence that UNC1151 is linked to the Belarusian government, whereas EU officials had earlier associated the Ghostwriter campaign with Russian state activity.[34] The strategic implication is plain. An intelligence operation need not begin with the penetration of a classified network; it may begin with a

[31] Ibid 16.

[32] AI Act, art 6(2) and Annex III, point 2. According to recital 55, components intended to be used solely for cybersecurity purposes do not qualify as safety components, so that an AI system deployed only to secure such infrastructure would not be classified as high-risk on that basis.

[33] CERT Polska (n 3).

[34] European Repository of Cyber Incidents (EuRepoC), 'Threat Profile: UNC1151' <https://strapi.eurepoc.eu/uploads/Eu_Repo_C_APT_profile_UNC_1151_fdbb22d127.pdf> accessed 1 October 2026; CyberScoop, 'Mandiant links Belarus to Ghostwriter campaign, which leaked stolen data and pushed disinformation' <https://cyberscoop.com/unc1151-belarus-russia-influence-ops/> accessed 1 October 2026; Dark Reading, 'Belarus Linked to Big European Disinformation Campaign' <https://www.darkreading.com/cyberattacks-data-breaches/report-identifies-belarus-involvement-in-big-european-disinformation-campaign> accessed 1 October 2026.

consultant, a supplier, a lawyer, a researcher, a personal mailbox, a subcontractor or an administrator holding comparatively mundane access. Hybrid conflict thus converts the extended enterprise into part of the national attack surface.

The healthcare breaches of 2026 illustrate concentration risk even more directly. On 12 August 2026 the Ministry of Digital Affairs confirmed unauthorised access to historical data, up to April 2024, of medical practices stored in the systems of MyDr, a provider of software for medical practices, potentially concerning 18.8 million people and more than 12,000 medical facilities.[35] In data protection terms MyDr acted as a processor, while the individual practices remained controllers.[36] The attacker did not need to breach twelve thousand facilities one by one; it sufficed to breach the processor to which they had entrusted their data. The President of the Personal Data Protection Office (UODO) ordered an inspection of the company covering the technical and organisational measures applied, including its risk analysis, and on 16 September 2026 decided to carry out additional inspections of the processing of health data until the end of 2026; by 17 September more than 50 complaints and over 2,000 breach notifications from controllers had been received in connection with the incident.[37] The immediate legal framework for these incidents is data protection and cybersecurity law rather than the AI Act, in particular the obligation of controllers to use only processors providing sufficient guarantees of appropriate technical and organisational measures, and the duty of controllers and processors to ensure a level of security appropriate to the risk.[38] Their relevance here lies in showing how aggregation changes the strategic value and the consequences of a compromise.

According to the government, the incident was criminal in origin: the Prime Minister stated that it appeared to have been motivated by an attempt to extort a ransom, and the Ministry

---

[35] Ministry of Digital Affairs, statement of 12 August 2026, quoted in 'Cyberatak na dane Polaków. Możesz zastrzec swój PESEL' (wroclaw.pl) <https://www.wroclaw.pl/dla-mieszkanca/cyberatak-na-dane-medyczne-polakow-przypominamy-jak-zastrzec-pesel> accessed 1 October 2026; Notes from Poland, 'Poland hit by theft of 19 million patients' data from medical platform' (13 August 2026) <https://notesfrompoland.com/2026/08/13/poland-hit-by-theft-of-19-million-patients-data-from-medical-platform/> accessed 1 October 2026.

[36] Interview with the President of the Personal Data Protection Office (UODO), conducted by J Kaczmarczyk, *Interia* (2026) <https://wydarzenia.interia.pl/kraj/news-kto-zaplaci-za-gigantyczny-wyciek-danych-polakow-prezes-uodo,nId,23531711> accessed 1 October 2026.

[37] UODO, 'Miliony Polaków poszkodowane. Po nowym wycieku danych medycznych PUODO zapowiada kontrolę' [Millions of Poles affected. Following a new medical data leak, the President of UODO announces an inspection] (25 September 2026) <https://uodo.gov.pl/pl/138/4585> accessed 1 October 2026.

[38] 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) (OJ L 119, 4.5.2016, p. 1), hereinafter: GDPR, art 28(1) and art 32(1).

indicated that foreign intelligence services were not behind it.[39] No foreign-state attribution may therefore be inferred. The President of UODO nevertheless observed that a leak of health data, particularly concerning public figures, may become an instrument of blackmail,[40] and the perpetrators reportedly demonstrated possession of the data by sending information about a prominent politician, including his PESEL number and details of prescriptions issued to him.[41] The case demonstrates that data collected for ordinary civilian purposes acquire intelligence value once aggregated at sufficient scale, regardless of who first extracts them.

The pattern did not end there. On 25 September 2026 UODO reported a new leak associated with the Medyc software of Qbusoft, which may concern the medical data of up to five million people, and announced an inspection of the provider. The authority quoted the Minister of Digital Affairs, according to whom security recommendations for healthcare software providers had been sent to suppliers on 16 September 2026 and the provider had not reported the incident to CERT Polska or to the healthcare sector CSIRT.[42] The scale of that incident had not been officially confirmed at the date of writing.[43] On 29 September 2026 the Ministry of Finance found it necessary to state publicly that a reported breach at Fakturownia.pl, a provider of invoicing software capable of connecting to the National e-Invoicing System (KSeF), did not concern data held in KSeF, and that its own verification had revealed no breach of the system's security.[44] Specialist media reported that the same perpetrators may stand behind the MyDr, Medyc and Fakturownia incidents, a claim not confirmed in the official communications cited above.[45]

---

[39] Polskie Radio, 'Major Polish data breach aimed at extorting ransom, PM says' (13 August 2026) <https://polskieradio.pl/395/7784/Artykul/3719734,major-polish-data-breach-aimed-at-extorting-ransom-pm-says> accessed 1 October 2026; money.pl, '„Nie zostały jeszcze nigdzie opublikowane". Minister o danych milionów Polaków' <https://www.money.pl/firma/wyciek-danych-19-mln-polakow-minister-o-tym-co-sie-stalo-z-danymi-7317741974063232a.html> accessed 1 October 2026.

[40] Interview (n 36).

[41] money.pl (n 39).

[42] UODO (n 37).

[43] Alert Medyczny, 'Możliwy wyciek danych z systemu Medyc. Prezes UODO skontroluje firmę Qbusoft' <https://alertmedyczny.pl/mozliwy-wyciek-danych-z-systemu-medyc-prezes-uodo-skontroluje-firme-qbusoft/> accessed 1 October 2026.

[44] Statement of the Ministry of Finance of 29 September 2026, quoted in pit.pl, 'Wyciek danych z Fakturownia.pl. Czy dotyczy danych zawartych w KSeF?' <https://www.pit.pl/efaktura/wyciek-danych-z-fakturownia-pl-czy-dotyczy-danych-zawartych-w-ksef> accessed 1 October 2026; Portal.Faktura.pl, 'Cyberatak na Fakturownia.pl. Firma potwierdza wyciek danych, KSeF bez naruszenia' <https://portal.faktura.pl/technologia/cyberatak-na-fakturownia-pl-firma-potwierdza-wyciek-danych-ksef-bez-naruszenia/> accessed 1 October 2026.

[45] Dobreprogramy, 'Gigantyczny wyciek danych z Fakturowni. Reagują resort finansów i służby' <https://www.dobreprogramy.pl/gigantyczny-wyciek-danych-z-fakturowni-reaguja-resort-finansow-i-sluzby,7334915118565632a> accessed 1 October 2026 (citing Zaufana Trzecia Strona); CyberDefence24,

The distinction drawn by the Ministry of Finance is itself instructive. In a digitally interconnected state, understanding an incident requires knowing not merely that 'a system' was breached, but where exactly the boundaries run between the supplier, the state platform, the processor, the controller, the cloud environment, the interface, the database and the downstream customer. Cybersecurity thus becomes an exercise in dependency topology.

5. Concentration of digital power: the provider as a security asset and a strategic attack surface

None of the foregoing establishes that large technology companies are inherently less secure than smaller providers, and the opposite will often be true. Hyperscalers and major technology corporations can invest in security engineering, threat intelligence, physical protection, cryptography, identity controls and incident response on a scale unavailable to an individual hospital, municipality or medium-sized enterprise. The problem is therefore not vendor quality as such but consequence multiplied by concentration. The more customers, identities, workloads and critical processes depend on the same provider, the greater the strategic return from compromising that provider or one of its privileged technological layers.

The SolarWinds operation demonstrated this logic. On 15 April 2021 the United States formally named the Russian Foreign Intelligence Service (SVR) as the perpetrator of the broad cyber-espionage campaign that exploited the SolarWinds Orion platform, stating that the compromise of the software supply chain had given the SVR the ability to spy on or potentially disrupt more than 16,000 computer systems worldwide.[46] The vector was the build environment of a trusted vendor, so that a legitimate update mechanism became a channel of initial access into many organisations at once.

Microsoft has itself been both a target and a conduit. In January 2024 it disclosed that the actor it tracks as Midnight Blizzard had used password spraying to compromise a legacy non-production test tenant account and had then used that account's permissions to access a small percentage of corporate mailboxes, including those of members of the senior leadership team and of employees in cybersecurity and legal functions. In March 2024 it reported that

'Wyciek danych Polaków z Medyc. Firma komentuje' <https://cyberdefence24.pl/cyberbezpieczenstwo/wycieki-danych/wyciek-danych-polakow-z-medyc-firma-komentuje> accessed 1 October 2026.

[46] National Counterintelligence and Security Center, 'SolarWinds Orion Software Supply Chain Attack' (last updated 19 August 2021) <https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/SolarWinds%20Orion%20Software%20Supply%20Chain%20Attack.pdf> accessed 1 October 2026; The Record, 'White House formally blames Russian intelligence service SVR for SolarWinds hack' <https://therecord.media/white-house-formally-blames-russian-intelligence-service-svr-for-solarwinds-hack> accessed 1 October 2026, quoting the White House statement of 15 April 2021.

information exfiltrated from those mailboxes had been used to gain access to some of its source code repositories and internal systems. The actor is publicly linked to the SVR.[47] In a separate case, an actor assessed to be affiliated with the People's Republic of China and known as Storm-0558 accessed the Exchange Online mailboxes of 22 organisations and more than 500 individuals using authentication tokens signed with a Microsoft consumer signing key created in 2016, which, combined with a flaw in Microsoft's authentication system, permitted access to enterprise accounts. The US Cyber Safety Review Board described a cascade of avoidable errors and a corporate culture that had deprioritised enterprise security investment and rigorous risk management, and noted that Microsoft did not know how or when the key had been obtained.[48]

Telecommunications display the same pattern at population scale. In April 2025 the FBI stated that the activity of PRC-affiliated actors publicly tracked as Salt Typhoon had compromised multiple US telecommunications companies and resulted in the theft of call data logs, of a limited number of private communications involving identified victims, and in the copying of select information subject to court-ordered law enforcement requests.[49] The last element deserves emphasis, since information generated by the machinery of lawful interception itself became an object of foreign collection. Even the tools of defence are nodes in the supply chain. In March 2026 attackers used stolen credentials to publish malicious versions of Aqua Security's Trivy vulnerability scanner and to repoint the tags of the associated GitHub Actions, in what was described as the continuation of a supply-chain attack that had begun in late February 2026; a public lookup released in August 2026 listed thousands of

---

[47] K Mackie, 'Microsoft Source Code Was Accessed by Midnight Blizzard Attackers' (*Redmond*, 8 March 2024) <https://redmondmag.com/articles/2024/03/08/microsoft-source-code-midnight-blizzard.aspx> accessed 1 October 2026; P Paganini, 'Russia-linked Midnight Blizzard breached Microsoft systems again' (*Security Affairs*, 8 March 2024) <https://securityaffairs.com/160207/hacking/russia-midnight-blizzard-breached-microsoft.html> accessed 1 October 2026; Help Net Security, 'Microsoft: Russian hackers accessed internal systems, code repositories' <https://www.helpnetsecurity.com/?p=294432> accessed 1 October 2026. The three sources report the statements of the Microsoft Security Response Center of 19 January and 8 March 2024.

[48] Lawfare, 'CSRB Lashes Microsoft's "Cascade of Security Failures" + Supply Chain Compromises' <https://lawfaremedia.org/article/csrb-lashes-microsoft-s-cascade-of-security-failures-supply-chain-compromises> accessed 1 October 2026; SC Media, 'Review board slams Microsoft's lax security practices and culture' <https://scworld.com/news/review-board-slams-microsofts-lax-security-practices-and-culture> accessed 1 October 2026; Computing, 'Microsoft's lax security blasted by investigators after serious breach' <https://computing.co.uk/news/4192192/microsofts-lax-security-blasted-investigators-breach> accessed 1 October 2026. The three sources summarise and quote the report of the Board released in April 2024.

[49] Federal Bureau of Investigation, 'FBI Seeking Tips about PRC-Targeting of US Telecommunications' (Public Service Announcement, 24 April 2025) <https://www.ic3.gov/PSA/2025/PSA250424-2>, text reproduced in HSToday, 'FBI Seeking Tips About PRC-Targeting of U.S. Telecommunications' <https://www.hstoday.us/subject-matter-areas/cybersecurity/fbi-seeking-tips-about-prc-targeting-of-u-s-telecommunications/> accessed 1 October 2026.

potentially affected organisations.[50] A scanner deployed to improve supply-chain security, and running by design with privileged access to the secrets of continuous integration pipelines, thus became a channel of compromise.[51] Compromises of software supply chains such as SolarWinds and Trivy fall primarily within the remit of the CRA and NIS2 rather than of the AI Act; they are better read as an argument for interoperability between these regimes than as a reproach to any single instrument.

These cases do not prove that concentration should be eliminated, nor that every affected organisation was negligent. They demonstrate something more fundamental, namely that strategic adversaries optimise for leverage. A supplier that opens the door to hundreds of customers is a natural target; so is an identity system that authenticates dozens of applications, and so is a telecommunications operator holding metadata at population scale. An environment that provides a semantic representation of an organisation's people, assets, relationships and operations necessarily belongs to that organisation's highest security tier.

Palantir deserves separate attention, because it sits at the intersection of data integration, analytics, artificial intelligence, defence, government and operational decision-making, and because it is an area in which legitimate criticism easily becomes technically imprecise. As of 1 October 2026 there is no reliable publicly available evidence that Russian intelligence or any other foreign intelligence service has taken control of Palantir's core platform. References to Palantir in this article do not imply that every Palantir product or deployment constitutes an AI system, let alone a high-risk AI system, within the meaning of the AI Act; classification depends on the characteristics and intended purpose of the specific system and deployment.[52] In its annual report filed on 17 February 2026 the company stated that its business strategy, results of operations and financial condition had not to date been materially affected by cybersecurity incidents, and described its information security team as experienced in managing threats including those from insiders and nation-state actors.[53] Public vulnerability records nonetheless

[50] CVE-2026-33634, record in the GCVE database <https://db.gcve.eu/vuln/CVE-2026-33634> accessed 1 October 2026; Docker, 'Trivy supply chain compromise: What Docker Hub users should know' (23 March 2026) <https://www.docker.com/blog/trivy-supply-chain-compromise-what-docker-hub-users-should-know/> accessed 1 October 2026; Barracuda Networks, 'Trivy Supply-Chain Compromise / CloudSEK Disclosure' (updated 24 August 2026) <https://trust.barracuda.com/security/information/trivy-supply-chain-compromise> accessed 1 October 2026.

[51] Legit Security, 'The Trivy Supply Chain Compromise: What Happened and Playbooks to Respond' <https://www.legitsecurity.com/blog/the-trivy-supply-chain-compromise-what-happened-and-playbooks-to-respond> accessed 1 October 2026.

[52] AI Act, arts 3(1) and 6.

[53] Palantir Technologies Inc., Annual Report on Form 10-K for the fiscal year ended 31 December 2025, Item 1C (Cybersecurity), filed 17 February 2026, as reproduced at <https://www.board-cybersecurity.com/annual-reports/20260217-palantir-technologies-item-1c-cybersecurity> accessed 1 October 2026.

show why platforms of this kind require exceptional assurance. CVE-2025-68609, published in January 2026 and corresponding to Palantir's defect identifier PLTRSEC-2025-53, concerned the Aries service on Apollo instances: in the default configuration both authentication and authorisation checks were bypassed, potentially allowing any network-accessible client to view system logs and perform operations without valid credentials, although no evidence of exploitation was identified during the vulnerability window.[54] CVE-2025-62487 concerned files uploaded through the Dossier application which, following a change introduced in May 2025, were not marked with the proper security levels on deployments without a CBAC configuration, on which no dialog prompts the user to set the security level of an upload, so that access to them was determined by default authorisation rules which on most environments add only the 'Everyone' group.[55] Defects of this kind are not evidence of hostile capture. They show, however, that in a platform whose value lies in integrating data under fine-grained access policies, configuration and authorisation errors translate directly into exposure.

Reports of a red-team exercise, published in 2016, in which the testers obtained very extensive internal privileges are sometimes cited without context. The exercise was commissioned by Palantir from Veris Group, and contemporaneous commentary noted that the leaked report also recorded strengths in Palantir's defences, including the response of its security staff, which the testers rated as excellent.[56] It was a security test performed on behalf of the company, not evidence of a hostile intelligence takeover. This distinction strengthens rather than weakens the argument about systemic risk. The pertinent question is not whether Palantir has already been secretly captured by a foreign service, for which there is no public evidentiary basis, but what the organisational consequence would be if a highly privileged data-integration and operational-decision platform were compromised. The question applies equally to Microsoft, Google, Amazon, Oracle, SAP, identity providers, telecommunications operators and any other platform occupying a sufficiently privileged position in critical organisational architecture. Robust controls do not remove systemic importance. The more extensively a

[54] National Vulnerability Database, 'CVE-2025-68609 Detail' <https://nvd.nist.gov/vuln/detail/CVE-2025-68609> accessed 1 October 2026; for the correspondence with defect PLTRSEC-2025-53 and the publication date of 22 January 2026 see the record in the GCVE database <https://db.gcve.eu/vuln/cve-2025-68609> accessed 1 October 2026.

[55] National Vulnerability Database, 'CVE-2025-62487 Detail' <https://nvd.nist.gov/vuln/detail/CVE-2025-62487> accessed 1 October 2026.

[56] BuzzFeed News, 'How Hired Hackers Got "Complete Control" of Palantir' (18 June 2016), as indexed at <https://social.cyware.com/news/how-hired-hackers-got-complete-control-of-palantir-c53bbac8> accessed 1 October 2026; Fortune, 'Here's What You Should Take Away From that "Palantir Hacked!" Story' (18 June 2016) <https://fortune.com/2016/06/18/palantir-hack-buzzfeed/> accessed 1 October 2026.

platform integrates an organisation, the greater the need to protect the integrity of its control plane, its identity plane, its data lineage and its administrative privileges.

6. The wider EU resilience architecture: DORA, NIS2, the CRA and the CER Directive

DORA starts from the premise that outsourcing technology does not outsource responsibility. Under Article 28(1)(a), financial entities that have contractual arrangements for the use of ICT services remain at all times fully responsible for compliance with, and the discharge of, all obligations under the Regulation and applicable financial services law. Before entering into an arrangement they must identify and assess all relevant risks, including the possibility that it may contribute to reinforcing ICT concentration risk, and for ICT services supporting critical or important functions they must put in place exit strategies, with exit plans that are comprehensive, documented, sufficiently tested and periodically reviewed.[57] Article 29 makes concentration an explicit object of assessment. Financial entities must consider whether a contemplated arrangement would lead to contracting a provider that is not easily substitutable, or to multiple arrangements for critical or important functions with the same provider or with closely connected providers. Where subcontracting of such functions is possible, they must weigh its benefits and risks, in particular where the subcontractor is established in a third country, and where the provider itself is established in a third country they must also consider compliance with Union data protection rules and the effective enforcement of the law in that country.[58] The last criterion introduces jurisdiction as a risk factor, which is precisely the factor that hybrid conflict renders salient.

The European Supervisory Authorities have operationalised concentration at the systemic level. On 18 November 2025 they designated critical ICT third-party providers on the basis of data drawn from the registers of information maintained by financial entities, after assessing each provider's systemic importance, its role in supporting critical or important functions and the substitutability of its services.[59] The list comprises primarily large cloud and platform providers.[60] The unit of analysis thereby changes. The question is no longer only whether Bank

[57] DORA, art 28(1)(a), (4)(c) and (8).

[58] DORA, art 29(1) and (2).

[59] European Supervisory Authorities (EBA, EIOPA and ESMA), 'The European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act' (18 November 2025) <https://www.esma.europa.eu/press-news/esma-news/european-supervisory-authorities-designate-critical-ict-third-party-providers> accessed 1 October 2026.

[60] PayTechLaw, 'European Supervisory Authorities publish list of critical ICT third-party providers' <https://paytechlaw.com/en/esas-publish-list-of-critical-ict-third%E2%80%91party-providers/> accessed 1

A manages Vendor X properly, but whether the simultaneous dependence of Banks A, B, C and D on Vendor X is itself a systemic problem.

NIS2 introduces a complementary logic. Article 21(1) requires essential and important entities to take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of their network and information systems. Under Article 21(2) those measures, based on an all-hazards approach, must include at least policies on risk analysis and information system security, incident handling, business continuity and crisis management, supply chain security including the relationships with direct suppliers and service providers, security in acquisition, development and maintenance including vulnerability handling and disclosure, procedures to assess the effectiveness of the measures, basic cyber hygiene and training, the use of cryptography, human resources security, access control and asset management, and multi-factor or continuous authentication. Article 21(3) requires entities to take into account the vulnerabilities specific to each direct supplier and the results of coordinated security risk assessments of critical supply chains carried out at Union level under Article 22.[61] The recitals go further. They point to the prevalence of incidents in which attackers compromised entities by exploiting vulnerabilities in third-party products and services, allow entities to consider risks stemming from other levels of suppliers, and single out managed security service providers as posing a particular risk because of their close integration in the operations of their clients.[62] DORA and NIS2 should not, however, be understood as cumulatively imposing identical obligations on financial entities. Article 4(1) NIS2 disapplies its relevant provisions, including those on supervision and enforcement, where sector-specific Union legal acts impose requirements at least equivalent in effect, and the Commission has identified DORA as such an act, so that the corresponding NIS2 provisions do not apply to financial entities within its scope.[63]

The adjective ‘organisational’ is crucial. A vulnerability is not only an entry in a vulnerability database. It may be an administrator with excessive standing privileges, an

October 2026, naming among the designated providers AWS, Google Cloud, Deutsche Telekom, Microsoft, Oracle and SAP.

[61] NIS2, art 21(1)-(3).

[62] NIS2, recitals 85 and 86; see also recital 83 on the application of the obligations regardless of whether systems are maintained internally or outsourced.

[63] NIS2, art 4(1); European Commission, Guidelines on the application of Article 4(1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive) (18 September 2023), CELEX 52023XC0918(01), Appendix; see EASA, ‘NIS2 guidelines on sector specific Union legal acts & Part-IS’ (29 September 2023) <https://www.easa.europa.eu/community/topics/nis2-guidelines-sector-specific-union-legal-acts-part> accessed 1 October 2026.

unmanaged subcontractor, an undocumented dependency, an unsupported device or a supplier for which no alternative exists. It may equally take the form of a security patch awaiting procurement approval, a contractual clause that prevents meaningful audit, a notification deadline longer than the time an attacker needs to exfiltrate the relevant environment, a recovery plan that has never been tested, privileged third-party access invisible to the customer's security operations centre, or a technically excellent supplier whose simultaneous failure would disable an entire sector. The Polish energy incidents illustrate the point concretely, since the decisive weaknesses lay in configuration choices and in responsibilities divided between operators, integrators and the distribution system operator. This is procedural vulnerability management, and it becomes indispensable once AI is embedded in critical processes rather than consumed as an isolated application.

National law has begun to draw the geopolitical consequences. The Polish Act of 23 January 2026 amending the Act on the National Cybersecurity System, in force since 3 April 2026, transposes NIS2 and, drawing on the EU 5G Toolbox, introduces a procedure for designating high-risk suppliers.[64] The designation takes the form of an administrative decision subject to review by the administrative courts, and equipment of a supplier so designated must be withdrawn from the systems of essential and important entities within periods ranging from four to seven years.[65] On signing the act, the President referred selected provisions concerning the procedure to the Constitutional Tribunal for follow-up review, which does not suspend their application.[66] Whatever the outcome of that review, the mechanism shows that the identity and jurisdiction of a supplier are already treated in national law as security variables. Both remain absent from the conformity logic of the AI Act.

The CRA adds the product layer. It lays down horizontal cybersecurity requirements for products with digital elements, requires manufacturers to exercise due diligence when integrating components sourced from third parties, including free and open-source components,

---

[64] Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw [Act of 23 January 2026 amending the Act on the National Cybersecurity System and certain other acts] (Dz.U. 2026, item 252); see the official ELI record <https://eli.gov.pl/eli/DU/2026/252/ogl> accessed 1 October 2026.

[65] Ministry of Digital Affairs, 'Sejm uchwalił nowelizację ustawy o Krajowym Systemie Cyberbezpieczeństwa' (23 January 2026) <https://www.gov.pl/web/cyfryzacja/sejm-uchwalil-nowelizacje-ustawy-o-krajowym-systemie-cyberbezpieczenstwa> accessed 1 October 2026; Bankier.pl, 'Sejm uchwalił nowelizację ustawy o krajowym systemie cyberbezpieczeństwa' (23 January 2026) <https://www.bankier.pl/wiadomosc/Sejm-uchwalil-nowelizacje-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-9073502.html> accessed 1 October 2026.

[66] Infor.pl, 'NIS2 wchodzi do Polski' <https://ksiegowosc.infor.pl/wiadomosci/7533605,nis2-wchodzi-do-polski-nawrocki-podpisal-ustawe-firmy-musza-dzialac-natychmiast-kary-siegna-10-mln-euro.html> accessed 1 October 2026.

and obliges them to identify and document the components of their products, including by drawing up a software bill of materials covering at least the top-level dependencies. Its stricter regime for important products extends, among others, to identity management systems and privileged access management software, products with virtual private network functions, routers and network management systems.[67] These categories correspond closely to the layers exploited in the cases discussed above: the VPN device and the router in the Polish energy sector, the build environment of a widely deployed IT management platform in the case of SolarWinds, and the release pipeline of a security scanner in the case of Trivy. The CRA applies in principle from 11 December 2027, while the reporting obligations of manufacturers under its Article 14 have applied since 11 September 2026.[68]

The CER Directive covers the entity layer of critical infrastructure and is, in an analysis of hybrid warfare, an even more natural point of reference than the AI Act. Member State risk assessments and the risk assessments carried out by critical entities must account for the relevant natural and man-made risks, expressly including hybrid threats and other antagonistic threats, and critical entities must take appropriate and proportionate technical, security and organisational measures, including measures to recover from incidents that duly consider business continuity and the identification of alternative supply chains.[69] The Directive disapplies these obligations, among others, for critical entities in the banking, financial market infrastructure and digital infrastructure sectors, whose resilience it leaves to DORA and NIS2 respectively.[70] A combined heat and power plant, a bank and the cloud provider serving both are thus governed by different instruments, each of which captures a different slice of the same dependency.

The blind spot is therefore not the absence of regulation, but the absence of a common dependency model connecting AI governance, product cybersecurity, entity-level cyber resilience, operational resilience and critical-infrastructure resilience. The AI Act addresses AI-specific risks to health, safety and fundamental rights; the CRA the cybersecurity of products; NIS2 the cyber resilience of entities; DORA the operational resilience of the financial sector;

---

[67] CRA (n 7), art 13(5), Annex I, Part II, point (1), and Annex III; see also the summary of the final act in the European Parliament's Legislative Observatory <https://oeil.europarl.europa.eu/oeil/en/document-summary?id=1796083> accessed 1 October 2026.

[68] Legislative Observatory (n 67); Hunton Andrews Kurth, 'Cyber Resilience Act Published in the Official Journal of the EU' <https://huntonak.com/privacy-and-information-security-law/cyber-resilience-act-published-in-the-official-journal-of-the-eu> accessed 1 October 2026.

[69] CER Directive (n 8), arts 5, 12 and 13(1)(d). Member States were to identify critical entities by 17 July 2026, and the obligations under Chapter III apply to them ten months after notification (art 6).

[70] CER Directive, art 8 and recitals 20 and 21.

the CER Directive the resilience of critical entities; the GDPR the security of personal data; and the Data Act[71] part of the problem of substitutability. A critical AI deployment cuts across all these layers at once, while Union law still lacks a common unit of analysis for the dependency graph as a whole.

7. From AI governance to AI operational resilience

An approach to critical AI infrastructure inspired by DORA, NIS2 and the wider resilience framework would not replace the AI Act, since it answers a different category of questions. The incidents examined above suggest three groups of control domains which together form an architecture of operational resilience for AI deployed in critical processes.

The first group concerns knowledge of dependencies. Organisations should be able to identify not only their direct AI provider but the entire critical dependency chain, including the cloud, the model provider, identity services, telecommunications, data services, managed security services, critical libraries and material subcontractors, and they should measure concentration at the level of the group and the sector rather than contract by contract. In the financial sector the registers of information required under DORA, which the European Supervisory Authorities already use to identify critical providers, supply the data model for such mapping.[72] Visibility must extend beyond the first tier. The security posture of a primary provider is insufficient if a fourth-party component can become a transitive compromise path, as the Trivy incident illustrates, and NIS2 already contemplates that entities may consider risks stemming from other levels of suppliers.[73] Knowledge of dependencies also comprises the analysis of data concentration. Risk assessments should examine not only whether each data set may lawfully be processed, but also what strategic information emerges once data sets are aggregated; the MyDr case shows that medical, financial, telecommunications and behavioural information may possess an intelligence value far exceeding that of each data set considered separately.

The second group concerns control over privileged access and the quality of assurance. Administrative access by the organisation, by the vendor and by its subcontractors should be treated as a distinct threat surface, governed by just-in-time privilege, segregation of duties,

[71] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data [...] (Data Act) (OJ L, 2023/2854, 22.12.2023), applicable from 12 September 2025.

[72] See n 59.

[73] NIS2, recital 85 (n 62).

hardware-backed authentication, logging independent of the environment that generates it and customer visibility of the provider's privileged actions. The incidents discussed above point in the same direction: a test tenant compromised through password spraying in the Midnight Blizzard case, a stolen signing key in the Storm-0558 case, a VPN accessible without multi-factor authentication and default credentials in the Polish energy sector, and the interception of one-time codes in the UNC1151 campaign, which suggests that phishing-resistant authentication should become the standard for high-value accounts. Supplier assurance, in turn, cannot rely on periodic questionnaires where strategic suppliers are concerned. It should incorporate continuous attack-surface assessment, penetration testing, red-team exercises, supply-chain compromise scenarios and intelligence on state-sponsored actors. The recommendation of CERT Polska to include private APNs and the devices providing access to them in penetration tests, red-team exercises and security architecture reviews is an example of assurance that follows the actual attack path rather than the contractual perimeter.[74]

The third group concerns the capacity to survive a loss of trust. A contractual right to terminate is not equivalent to technical substitutability. Exit planning requires the portability of data, configuration, audit records and relevant model artefacts, documented migration paths, alternative capacity and periodic testing, which DORA already demands for ICT services supporting critical or important functions.[75] Outside the financial sector the Data Act adds a further component, since it requires providers of data processing services to remove pre-commercial, commercial, technical, contractual and organisational obstacles to switching to another provider, to on-premises ICT infrastructure or to the simultaneous use of several providers, and to publish information on the jurisdiction to which their ICT infrastructure is subject and on the measures taken to prevent international governmental access to non-personal data held in the Union.[76] It addresses portability and lock-in rather than operational resilience as such, but it bears directly on the substitutability dimension of dependency risk. Organisations should also rehearse the assumption that a trusted supplier has itself been compromised. SolarWinds demonstrated that this is not an exotic scenario, and an exercise built upon it should test whether the organisation is able to detect the compromise, isolate the supplier, revoke trust, reconstruct identity and continue critical operations. Operational resilience may, finally, be

[74] CERT Polska, Supplement (n 29) 16-17.

[75] DORA, art 28(8) (n 57).

[76] Data Act (n 71), arts 23 and 28(1); on the latter provision see CMS, 'Data Act and Cloud Service Providers (Part 1): Contract drafting and information obligations' <https://cms.law/en/deu/legal-updates/data-act-and-cloud-service-providers-part-1-contract-drafting-and-information-obligations> accessed 1 October 2026.

affected not only by cyberattacks but also by sanctions, export restrictions, armed conflict, changes in the law, government orders, loss of connectivity and political fragmentation. Technological concentration thus becomes part of geopolitical risk management rather than of procurement alone, and DORA's criterion of effective law enforcement in third countries, together with national procedures concerning high-risk suppliers, provides the legal anchor for such analysis.[77]

None of these mechanisms presupposes that major technology providers are untrustworthy. They rest on an orthodox principle of risk management: the greater the consequence of failure, the less acceptable unexamined trust becomes. The regulatory debate on artificial intelligence still concentrates on models, that is, on bias, hallucination, transparency, explainability, training data, copyright, human oversight and evaluation. These questions matter, but the most consequential AI security incident of the coming years may involve none of them. It may instead involve an authentication token, a compromised administrator, a poisoned software dependency, an update server, a forgotten interface, a telecommunications provider, a cloud control plane, a contractor with legitimate access or a single strategically positioned provider shared by hundreds of institutions. Regulating the model while neglecting the dependency architecture resembles certifying an aircraft while ignoring the airport, the fuel supply, the maintenance contractor, air traffic control and the identity of the person entering the cockpit. The aircraft may be fully compliant while the system is compromised.

8. Conclusions

The AI Act is an important development in European technology law because it recognises that artificial intelligence generates risks that call for ex ante governance rather than ex post liability alone. Its limitation does not lie in regulating too much or too little in some abstract sense. It lies in the fact that it regulates a particular conception of AI risk, centred on the system and its design, which Article 9(3) makes explicit.[78] The current security environment requires a second conception alongside the first, and Union law already contains its elements, dispersed across DORA, NIS2, the CRA, the CER Directive, the GDPR and the Data Act.

Europe faces documented Russian state and proxy cyber activity, espionage attributed to other states, destructive attacks against critical infrastructure, recurring exploitation of strategic technology suppliers and breaches capable of exposing millions of citizens at once. Not every

[77] DORA, art 29(2) (n 58); see Section 6 above.

[78] AI Act, art 9(3) (n 10).

cyber incident constitutes hybrid warfare, and attribution must remain evidence-based; the MyDr breach, criminal in origin according to the government, is a reminder of that. The incidents nonetheless establish that technological architecture can no longer be separated from national resilience, because data and access acquired for any motive can be redirected to strategic ends.

The concept of technofascism is analytically useful on the condition that it is not reduced to an insult. The danger it identifies is not that governments use artificial intelligence, but that informational concentration, technological concentration and political power become mutually reinforcing. A democratic state may legitimately build powerful technological capabilities, and a private corporation may legitimately supply them. Resilient democratic architecture, however, assumes that people, institutions and governments are fallible, and therefore limits irreversible concentrations of power. Architectural separation, least privilege, auditability, portability, redundancy, substitutability and the ability to revoke trust are the technical counterparts of constitutional checks and balances.

This is the deeper lesson of the resilience instruments discussed above. Cyber resilience cannot be purchased from a technology supplier, nor is it synonymous with encryption, penetration testing or certification; it is a governance process for managing dependency under conditions of uncertainty. Two conclusions de lege ferenda follow. First, the regulatory response need not consist in expanding the AI Act into a general cybersecurity or operational-resilience statute. A more coherent solution would require critical AI deployments to maintain a cross-regulatory dependency map linking the technical documentation under the AI Act to the applicable NIS2 or DORA risk registers, to CRA product dependencies, to CER resilience assessments and, where relevant, to Data Act switching capabilities, so that the regimes describe the same architecture rather than different abstractions of it. Second, the period until 2 December 2027, during which the requirements for Annex III high-risk systems do not yet apply, should be used to reflect such mapping, together with supplier-compromise scenarios, in the harmonised standards and in the Commission guidelines provided for in Article 96(1)(a), as amended in 2026, which cover the application of Articles 8 to 15, 25 and 26, building on the reference in recital 65 to risks arising from the interaction between the AI system and its environment, so that the limitation in Article 9(3) does not leave the deployment environment outside the field of view.[79]

[79] Article 96(1)(a) AI Act as replaced by art 1, point 36(a), of Regulation (EU) 2026/1744 (n 1).

The strategic question for the next generation of European AI governance is therefore broader than whether a given AI system is safe enough to use. It is who can control the system, who can compromise those who control it, which other systems depend on the same provider, whether that dependency can be independently verified, whether trust can be revoked, and whether the institution, and ultimately the state, can continue to function when the answer to one of those questions becomes uncomfortable. That is no longer AI compliance alone. It is technological sovereignty.

Bibliography

All online sources were accessed on 1 October 2026.

Legislation

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) (OJ L 333, 27.12.2022, p. 80).

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 (OJ L 333, 27.12.2022, p. 164).

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) (OJ L 119, 4.5.2016, p. 1).

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector [...] (OJ L 333, 27.12.2022, p. 1).

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data [...] (Data Act) (OJ L, 2023/2854, 22.12.2023).

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence [...] (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024).

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 and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024).

Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) (OJ L, 2026/1744, 24.7.2026).

Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw [Act of 23 January 2026 amending the Act on the National Cybersecurity System and certain other acts] (Dz.U. 2026, item 252) <https://eli.gov.pl/eli/DU/2026/252/ogl>.

Official documents, reports and statements

CERT-EU, ‘Cyber Brief 26-08: July 2026’ <https://cert.europa.eu/publications/threat-intelligence/cb26-08>.

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

CERT Polska, ‘Raport z incydentu w sektorze energii z 29 grudnia 2025 roku’ (30 January 2026) <https://cert.pl/posts/2026/01/raport-incydent-sektor-energii-2025/>.

CERT Polska, *Uzupełnienie raportu z incydentu w sektorze energii 29 grudnia 2025* (2026) <https://cert.pl/uploads/docs/CERT_Polska_Uzupelnienie_Raportu_Incydent_Sektor_Energii_2025.pdf>.

CERT Polska, ‘UNC1151/Ghostwriter phishing campaign targeting Gmail accounts’ (12 June 2026) <https://cert.pl/en/posts/2026/06/UNC1151-gmail-campaign/>.

Council of the European Union, ‘Cyber / Russia: Statement by the High Representative on behalf of the European Union denouncing Russia’s malicious cyber ecosystem targeting the EU, its member states and international partners’ (press release, 13 July 2026) <https://www.consilium.europa.eu/en/press/press-releases/2026/07/13/cyber-russia-statement-by-the-high-representative-on-behalf-of-the-european-union-denouncing-russia-s-malicious-cyber-ecosystem-targeting-the-eu-its-member-states-and-international-partners/>.

European Commission, AI Act Service Desk, text of Regulation (EU) 2024/1689, arts 2 and 9 <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-2>; <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-9>.

European Commission, ‘Guidelines on the application of Article 4(1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive)’ (18 September 2023), CELEX 52023XC0918(01).

European Parliament, Legislative Observatory, summary of the final act in procedure 2022/0272(COD) (Cyber Resilience Act) <https://oeil.europarl.europa.eu/oeil/en/document-summary?id=1796083>.

European Repository of Cyber Incidents (EuRepoC), ‘Threat Profile: UNC1151’ <https://strapi.eurepoc.eu/uploads/Eu_Repo_C_APT_profile_UNC_1151_fdbb22d127.pdf>.

European Supervisory Authorities (EBA, EIOPA and ESMA), ‘The European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act’ (18 November 2025) <https://www.esma.europa.eu/press-news/esma-news/european-supervisory-authorities-designate-critical-ict-third-party-providers>.

Federal Bureau of Investigation, ‘FBI Seeking Tips about PRC-Targeting of US Telecommunications’ (Public Service Announcement, 24 April 2025) <https://www.ic3.gov/PSA/2025/PSA250424-2>.

Future of Life Institute, AI Act Explorer, official text of Regulation (EU) 2026/1744 (Digital Omnibus on AI) <https://artificialintelligenceact.eu/ai-act-explorer/digital-omnibus/>.

Future of Privacy Forum, ‘EU AI Act Implementation Timeline (updated following the AI Omnibus)’ (July 2026) <https://fpf.org/wp-content/uploads/2026/07/FPF-EU-AI-Act-Timeline-2026-R2.pdf>.

GCVE database, records CVE-2025-68609 <https://db.gcve.eu/vuln/cve-2025-68609> and CVE-2026-33634 <https://db.gcve.eu/vuln/CVE-2026-33634>.

Ministry of Digital Affairs, ‘Sejm uchwalił nowelizację ustawy o Krajowym Systemie Cyberbezpieczeństwa’ (23 January 2026) <https://www.gov.pl/web/cyfryzacja/sejm-uchwalil-nowelizacje-ustawy-o-krajowym-systemie-cyberbezpieczenstwa>.

National Counterintelligence and Security Center, ‘SolarWinds Orion Software Supply Chain Attack’ (last updated 19 August 2021) <https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/SolarWinds%20Orion%20Software%20Supply%20Chain%20Attack.pdf>.

National Vulnerability Database, ‘CVE-2025-62487 Detail’ <https://nvd.nist.gov/vuln/detail/CVE-2025-62487>.

National Vulnerability Database, ‘CVE-2025-68609 Detail’ <https://nvd.nist.gov/vuln/detail/CVE-2025-68609>.

Palantir Technologies Inc., Annual Report on Form 10-K for the fiscal year ended 31 December 2025, Item 1C (Cybersecurity), filed 17 February 2026, as reproduced at <https://www.board-cybersecurity.com/annual-reports/20260217-palantir-technologies-item-1c-cybersecurity>.

Urząd Ochrony Danych Osobowych (UODO), ‘Miliony Polaków poszkodowane. Po nowym wycieku danych medycznych PUODO zapowiada kontrolę’ (25 September 2026) <https://uodo.gov.pl/pl/138/4585>.

Literature

Coeckelbergh M, ‘Technofascism: AI, Big Tech, and the New Authoritarianism’ *AI & Society* (published online 25 January 2026) <https://doi.org/10.1007/s00146-026-02862-9>.

Farrell H and Newman AL, ‘Weaponized Interdependence: How Global Economic Networks Shape State Coercion’ (2019) 44(1) *International Security* 42-79.

Roberts T and Oosterom M, ‘Digital Authoritarianism: A Systematic Literature Review’ *Information Technology for Development* (2024).

Vogiatzoglou P, ‘The AI Act National Security Exception: Room for Manoeuvres?’ (*Verfassungsblog*, 9 December 2024) <https://verfassungsblog.de/the-ai-act-national-security-exception/>, DOI 10.59704/292082becc7cc8e6.

Press and other online sources

Alert Medyczny, ‘Możliwy wyciek danych z systemu Medyc. Prezes UODO skontroluje firmę Qbusoft’ <https://alertmedyczny.pl/mozliwy-wyciek-danych-z-systemu-medyc-prezes-uodo-skontroluje-firme-qbusoft/>.

Bankier.pl, ‘Sejm uchwalił nowelizację ustawy o krajowym systemie cyberbezpieczeństwa’ (23 January 2026) <https://www.bankier.pl/wiadomosc/Sejm-uchwalil-nowelizacje-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-9073502.html>.

Barracuda Networks, ‘Trivy Supply-Chain Compromise / CloudSEK Disclosure’ (updated 24 August 2026) <https://trust.barracuda.com/security/information/trivy-supply-chain-compromise>.

BuzzFeed News, ‘How Hired Hackers Got “Complete Control” of Palantir’ (18 June 2016), as indexed at <https://social.cyware.com/news/how-hired-hackers-got-complete-control-of-palantir-c53bbac8>.

CMS, ‘Data Act and Cloud Service Providers (Part 1): Contract drafting and information obligations’ <https://cms.law/en/deu/legal-updates/data-act-and-cloud-service-providers-part-1-contract-drafting-and-information-obligations>.

Computing, ‘Microsoft’s lax security blasted by investigators after serious breach’ <https://computing.co.uk/news/4192192/microsofts-lax-security-blasted-investigators-breach>.

CyberDefence24, ‘Wyciek danych Polaków z Medyc. Firma komentuje’ <https://cyberdefence24.pl/cyberbezpieczenstwo/wycieki-danych/wyciek-danych-polakow-z-medyc-firma-komentuje>.

CyberScoop, ‘Mandiant links Belarus to Ghostwriter campaign, which leaked stolen data and pushed disinformation’ <https://cyberscoop.com/unc1151-belarus-russia-influence-ops/>.

Dark Reading, ‘Belarus Linked to Big European Disinformation Campaign’ <https://www.darkreading.com/cyberattacks-data-breaches/report-identifies-belarus-involvement-in-big-european-disinformation-campaign>.

Dobreprogramy, ‘Gigantyczny wyciek danych z Fakturowni. Reagują resort finansów i służby’ <https://www.dobreprogramy.pl/gigantyczny-wyciek-danych-z-fakturowni-reaguja-resort-finansow-i-sluzby,7334915118565632a>.

Docker, ‘Trivy supply chain compromise: What Docker Hub users should know’ (23 March 2026) <https://www.docker.com/blog/trivy-supply-chain-compromise-what-docker-hub-users-should-know/>.

EASA, ‘NIS2 guidelines on sector specific Union legal acts & Part-IS’ (29 September 2023) <https://www.easa.europa.eu/community/topics/nis2-guidelines-sector-specific-union-legal-acts-part>.

Fortune, ‘Here’s What You Should Take Away From that “Palantir Hacked!” Story’ (18 June 2016) <https://fortune.com/2016/06/18/palantir-hack-buzzfeed/>.

Help Net Security, ‘Microsoft: Russian hackers accessed internal systems, code repositories’ <https://www.helpnetsecurity.com/?p=294432>.

HSToday, ‘FBI Seeking Tips About PRC-Targeting of U.S. Telecommunications’ <https://www.hstoday.us/subject-matter-areas/cybersecurity/fbi-seeking-tips-about-prc-targeting-of-u-s-telecommunications/>.

Hunton Andrews Kurth, ‘Cyber Resilience Act Published in the Official Journal of the EU’ <https://huntonak.com/privacy-and-information-security-law/cyber-resilience-act-published-in-the-official-journal-of-the-eu>.

Infor.pl, ‘NIS2 wchodzi do Polski’ <https://ksiegowosc.infor.pl/wiadomosci/7533605,nis2-wchodzi-do-polski-nawrocki-podpisal-ustawe-firmy-musza-dzialac-natychmiast-kary-siegna-10-mln-euro.html>.

Interia, interview with the President of the Personal Data Protection Office, conducted by J Kaczmarczyk (2026) <https://wydarzenia.interia.pl/kraj/news-kto-zaplaci-za-gigantyczny-wyciek-danych-polakow-prezes-uodo,nId,23531711>.

ITwiz, ‘Za grudniowym atakiem na polską energetykę stoi rosyjska grupa Sandworm’ <https://itwiz.pl/?p=69814>.

Lawfare, ‘CSRB Lashes Microsoft’s “Cascade of Security Failures” + Supply Chain Compromises’ <https://lawfaremedia.org/article/csrb-lashes-microsoft-s-cascade-of-security-failures-supply-chain-compromises>.

Legit Security, ‘The Trivy Supply Chain Compromise: What Happened and Playbooks to Respond’ <https://www.legitsecurity.com/blog/the-trivy-supply-chain-compromise-what-happened-and-playbooks-to-respond>.

Mackie K, ‘Microsoft Source Code Was Accessed by Midnight Blizzard Attackers’ (*Redmond*, 8 March 2024) <https://redmondmag.com/articles/2024/03/08/microsoft-source-code-midnight-blizzard.aspx>.

money.pl, ‘„Nie zostały jeszcze nigdzie opublikowane”. Minister o danych milionów Polaków’ <https://www.money.pl/firma/wyciek-danych-19-mln-polakow-minister-o-tym-co-sie-stalo-z-danymi-7317741974063232a.html>.

Notes from Poland, ‘Poland hit by theft of 19 million patients’ data from medical platform’ (13 August 2026) <https://notesfrompoland.com/2026/08/13/poland-hit-by-theft-of-19-million-patients-data-from-medical-platform/>.

Paganini P, ‘Russia-linked Midnight Blizzard breached Microsoft systems again’ (*Security Affairs*, 8 March 2024) <https://securityaffairs.com/160207/hacking/russia-midnight-blizzard-breached-microsoft.html>.

PayTechLaw, ‘European Supervisory Authorities publish list of critical ICT third-party providers’ <https://paytechlaw.com/en/esas-publish-list-of-critical-ict-third%E2%80%91party-providers/>.

pit.pl, ‘Wyciek danych z Fakturownia.pl. Czy dotyczy danych zawartych w KSeF?’ <https://www.pit.pl/efaktura/wyciek-danych-z-fakturownia-pl-czy-dotyczy-danych-zawartych-w-ksef>.

Polskie Radio, ‘Major Polish data breach aimed at extorting ransom, PM says’ (13 August 2026) <https://polskieradio.pl/395/7784/Artykul/3719734,major-polish-data-breach-aimed-at-extorting-ransom-pm-says>.

Portal.Faktura.pl, ‘Cyberatak na Fakturownia.pl. Firma potwierdza wyciek danych, KSeF bez naruszenia’ <https://portal.faktura.pl/technologia/cyberatak-na-fakturownia-pl-firma-potwierdza-wyciek-danych-ksef-bez-naruszenia/>.

SC Media, ‘Review board slams Microsoft’s lax security practices and culture’ <https://scworld.com/news/review-board-slams-microsofts-lax-security-practices-and-culture>.

SecurityWeek, ‘Novel Private APN Pivot Let Hackers Sabotage Second Polish Energy Facility’ <https://www.securityweek.com/novel-private-apn-pivot-let-hackers-sabotage-second-polish-energy-facility/amp/>.

The Record, ‘White House formally blames Russian intelligence service SVR for SolarWinds hack’ <https://therecord.media/white-house-formally-blames-russian-intelligence-service-svr-for-solarwinds-hack>.

wroclaw.pl, ‘Cyberatak na dane Polaków. Możesz zastrzec swój PESEL’ <https://www.wroclaw.pl/dla-mieszkanca/cyberatak-na-dane-medyczne-polakow-przypominamy-jak-zastrzec-pesel>.