About the Article

Which EU critical infrastructure sectors face the greatest cyber risk, and which threat modalities are most active? The EU threat environment is bifurcated: high-volume DDoS/hacktivism pressures availability, while lower-volume intrusions cause high-consequence outcomes like ransomware and data theft.
Public administration, transport, digital infrastructure, finance, energy, and health are most at risk due to dependency entanglement, strategic importance, and recovery challenges.

About the Author

Sean is currently pursuing a Master's degree in International Security from Charles University, with a focus on Security and Technology. His research focuses on Machine Learning and analyzing current LLM vulnerabilities and their use by malicious actors. He is currently working on a Thesis project looking into the robustness of LLM RAG pipelines under adversarial conditions. His mission is to provide better guidance and research into cybersecurity surrounding the expanding AI market.

1. Introduction

Cyberattacks against EU critical infrastructure are best analysed as continuous pressure on interconnected systems, not as episodic "incidents." Essential services depend on shared digital enablers, identity, cloud and hosting, remote administration, managed service providers (MSPs), and software supply chains, so high-impact disruption often occurs without direct industrial control system (ICS) compromise. ENISA's 2025 threat landscape frames the environment as "more continuous, diversified and convergent campaigns that collectively erode resilience," rather than a small number of discrete, headline incidents. (ENISA ETL 2025) The 2024-2025 period is a particularly relevant window: NIS2 entered full enforcement in October 2024, and sustained geopolitical pressure from the Russia-Ukraine conflict has directly driven the hacktivist surge that now dominates EU incident volumes.

"Critical infrastructure" is anchored to the EU's NIS2-expanded perimeter, including energy, transport, healthcare, finance, water, digital infrastructure, and public services.

This report assesses the scale and scope of cyberattacks affecting EU infrastructure. The central argument is that the EU faces a bifurcated threat environment: (1) high-volume availability pressure dominated by DDoS and hacktivism, and (2) lower-volume but higher-consequence intrusions that convert into ransomware, data theft, and persistence, often via identity compromise, exposed edge services, and third-party dependencies. (ENISA ETL 2024; ENISA ETL 2025; Verizon DBIR 2025 Executive Summary) This raises the central research question: which sectors of EU critical infrastructure face the greatest risk, and which threat modalities are most active against them? The analysis is bounded by the NIS2 sector perimeter; it excludes classified or non-public incident data, does not address member-state-level variance in reporting obligations, and does not cover cyber-physical incidents outside that perimeter.

This report contributes to comparative infrastructure vulnerability literature by applying a systems-view, dependency-mediated framing rather than single-metric incident counts; a gap in most single-source threat intelligence outputs. In practice, the findings directly bear on NIS2 implementation: member states and operators allocating defensive resources can use the sector-risk map produced here to prioritise interventions. Security researchers, policymakers, and infrastructure operators are the primary intended audience. This report uses a literature review and synthesis methodology, drawing on open-source threat intelligence published in 2024-2025 and triangulated across multiple independent sources to control for reporting-visibility bias. Existing single-source reports (ENISA, Verizon, Sophos) each cover portions of this landscape; this report synthesises them into a cross-sector, dependency-aware risk map.

2. What is Critical Infrastructure?

To avoid definitional drift, "critical infrastructure" is anchored to the EU's NIS2-expanded perimeter of critical sectors including energy, transport,

finance, water management, digital infrastructure, public electronic communications, waste/wastewater management, postal/courier services, public administration, and space. (European Commission, NIS2 policy page) Sector labels remain an approximation: attackers frequently target cross-sector dependencies (identity, edge access, and third parties). (Verizon DBIR 2025 Executive Summary; ENISA ETL 2025) A practical implication is that infrastructure disruption is often dependency-mediated. A "transport" disruption may originate in an upstream IT provider; a "public administration" incident may stem from identity compromise; and a "health" disruption may spread through a shared platform. This report therefore prioritises a systems view: which sectors are most frequently targeted, which are most disruption-sensitive, and which sit at chokepoints that amplify cascades.

Highest-Risk Critical Infrastructure

- **Public administration** is the most consistently pressured target: it is the default focal point for high-visibility DDoS pressure and remains a high-value target for strategic intrusion and espionage. (ENISA ETL 2024; ENISA ETL 2025)
- **Transport and logistics** are among the most disruption-sensitive: incidents produce immediate operational effects and are increasingly mediated by vendor/platform chokepoints. (ENISA ETL 2025; Reuters, 22 Sep 2025)
- **Digital infrastructure and communications** are the systemic layer: compromise/disruption here cascades across dependent sectors and provides strategic leverage. (ENISA ETL 2024; CERT-EU TLR2024)
- **Finance** is both a target for availability pressure and over-represented among high-impact incident reporting. (ENISA ETL 2025)
- **Energy/utilities and health** are high-consequence extortion targets: disruption is costly, recovery burdens are high, and downtime tolerance is low even when the initial compromise is only IT. (Sophos CI Ransomware 2024; The Record, 13 Feb 2024; AP, 19 Dec 2025)

Public administration is the most consistently pressured target: it is the default focal point for high-visibility DDoS pressure and remains a high-value target for strategic intrusion and espionage

3. Measuring scale: triangulating incident volume, background pressure, and high-impact outcomes

"Scale" cannot be reduced to a single incident count because measurement regimes observe different portions of the threat surface. A defensible approach is to treat scale as a composite of: (i) incident tempo, (ii) cross-border reach, (iii) background attack pressure on identity and internet-exposed services, and (iv) the conversion rate from intrusion to operational disruption.

At the EU situational-awareness layer, ENISA observed 11,079 incidents in July 2023–June 2024, including 322 incidents targeting two or

more EU Member States. (ENISA ETL 2024) This establishes a baseline: the EU operates in a high-tempo environment with a recurring cross-border component. ENISA also cautions that OSINT-driven counts are shaped by reporting visibility and media attention, so they are best treated as indicators of tempo and pattern rather than a census. (ENISA ETL 2024)

For July 2024–June 2025, ENISA analyses 4,875 incidents using a more threat-centric approach and notes that open sources and voluntary sharing do not provide a complete picture. (ENISA ETL 2025) ENISA's 2025 distribution is dominated by DDoS (76.7%), followed by intrusions (17.8%). (ENISA ETL 2025) This supports the idea that availability disruption drives incident workload and public visibility, while intrusion activity is the primary pipeline to ransomware, data theft, and persistence.

A critical implication for scale is time lag. ENISA notes that ransomware and DDoS attacks are visible and often claimed quickly, whereas cyberespionage campaigns are typically documented with delays ranging from six months to more than four years. (ENISA ETL 2025) This means near-real-time incident tallies systematically undercount the activity most relevant to strategic infrastructure risk (prepositioning and stealth intrusion).

Beyond EU incident lists, "scale" must include the background pressure on infrastructure dependency layers. Microsoft reports more than 600 million attacks per day across its ecosystem and states that password-based attacks account for >99% of daily identity attacks, with Microsoft blocking 7,000 password attacks per second the past year. (Microsoft Digital Defense Report 2024) It also reports mitigating 1.25 million DDoS attacks in the second half of 2024. (Microsoft Digital Defense Report 2024) These figures are not EU-only incident counts, but they quantify the ambient contest over identity and availability that infrastructure operators must treat as continuous operating conditions.

Finally, scale becomes policy-relevant when hostile activity converts into restoration costs and downtime. Verizon's 2025 DBIR executive summary (global but applicable to EU operator risk) highlights the operational bottlenecks that sustain scalable compromise: edge devices and VPNs comprise 22% of vulnerability exploitation targets, only ~54% of those edge vulnerabilities were fully remediated through the year, and the median remediation time was 32 days. (Verizon DBIR 2025 Executive Summary) Combined with ENISA's findings on exploitation-to-intrusion conversion (Section 6), this supports a strong scale claim: infrastructure exposure is not only a function of attacker volume; it is amplified by patch latency at the edge and dependency entanglement.

4. Threat actor ecology and campaign logic: three actor classes, convergent effects

Threat actors differ in objectives, but their operational effects align on the same dependency surfaces; availability, identity, edge services, and third parties. ENISA reports that EU-targeting activities "mostly pertained to ideology-driven incidents" carried out by hacktivists through DDoS, while financially motivated operations were primarily carried out by cybercriminal operators; cyberespionage campaigns accounted

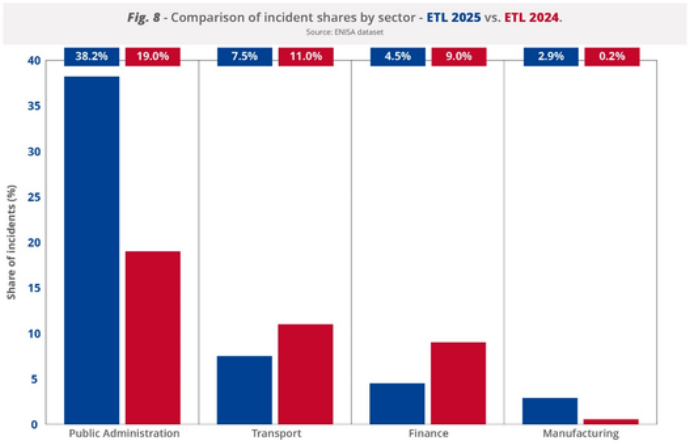
for 7.2% of assessed objectives. (ENISA ETL 2025) This creates a division of labour:

- Hacktivists drive tempo and visibility via DDoS pressure operations, and to a lesser extent defacements. Their primary infrastructure effect is service degradation and reputational pressure. (ENISA ETL 2025)
- Cybercriminals drive disruption and monetisation via intrusion outcomes, data theft, extortion, and ransomware deployment, supported by an access economy. Europol's IOCTA 2025 describes active markets for compromised access and data, including the role of initial access brokers, enabling downstream actors to turn access into ransomware and coercive disruption. (Europol IOCTA 2025)
- State-aligned actors drive persistence and leverage (espionage and prepositioning), typically detected later and often targeting upstream providers to maximise downstream access. (ENISA ETL 2025; CERT-EU TLR2024)

The practical infrastructure conclusion is that "actor labels" do not map cleanly onto defensive impact. Infrastructure defenders experience a messy environment: DDoS waves generate continuous load and visibility, while exploit/credential-driven intrusions generate the highest-consequence outcomes. This convergence is one reason incident counts can be misleading as measures of strategic risk.

5. Sectoral scope: where attacks concentrate and why

Sector targeting in EU infrastructure is broad but patterned: adversaries concentrate on (i) high-visibility public services where disruption is immediately observable and politically salient, (ii) systemic dependency layers where disruption cascades.



Source: ENISA Threat Landscape 2025

Public administration is the clearest "most targeted" sector. ENISA identifies public administration as the most targeted sector in 2024 (19% of observed events). (ENISA ETL 2024) DDoS disproportionately targets public administration: 33% of DDoS events were against public administration, followed by transport (21%), banking (12%), and digital infrastructure (6%).
(ENISA ETL 2024) In 2025, public administration accounts for 38% of incidents, and ENISA attributes 96.2% of the public administration threat picture to hacktivist-led DDoS. (ENISA ETL 2025) Infrastructure-relevant interpretation: public administration is the default target for "first-line" availability pressure around salient events, but it is also a high-value strategic target due to intelligence value and procurement/contractor ecosystem access. (ENISA ETL 2025)

Transport and logistics are central because disruption is immediate and cross-border. ENISA reports transport accounts for 7.5% of recorded incidents in 2025 and that 12% of significant-impact incidents reported under the NIS directive

in 2024 were transport incidents; within the sector, incidents concentrate in air transport (58.4%) and logistics (20.8%). (ENISA ETL 2025) While hacktivist DDoS dominates volume, ransomware is disproportionately disruptive. ENISA cites an incident at Split Airport linked to Akira ransomware that disrupted passenger reception information systems and led to a temporary suspension of flights. (ENISA ETL 2025) The sector is also increasingly exposed to vendor chokepoints: Reuters reports that a cyberattack affecting a third-party check-in/boarding systems provider disrupted multiple European airports; Brussels Airport cancelled 60 of 550 scheduled flights in one day and reverted to manual workflows as systems were restored. (Reuters, 22 Sep 2025) This is a dependency-cascade pattern: one compromised service node can create multi-airport operational impact.

Digital infrastructure and communications represent systemic multiplier risk. Digital infrastructure accounts for a substantial share of observed events in ENISA's 2024 dataset (8%) and is materially represented across malware, social engineering, and availability disruptions. (ENISA ETL 2024) CERT-EU's 2024 threat landscape notes service providers (telecoms, cybersecurity firms, remote access providers) as prime targets, consistent with a strategic adversary logic seeking upstream access and maximum downstream leverage. (CERT-EU TLR2024) Infrastructure relevance: attacks here can create multi-sector degradation and can enable downstream compromise at scale.

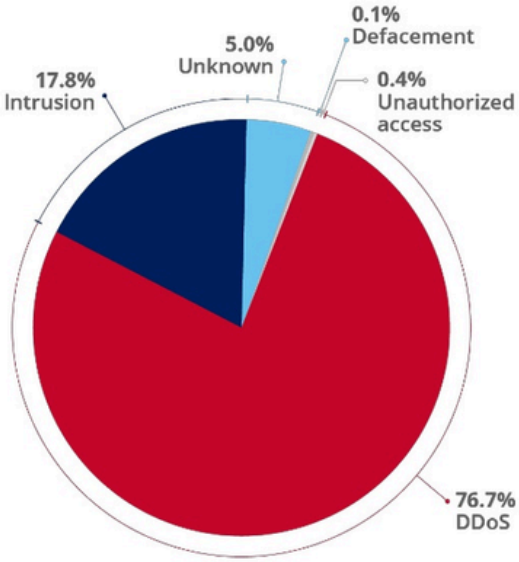
Finance combines targeting with trust externalities. In 2025, ENISA reports finance accounts for 4.7% of collected incidents, with hacktivist-led DDoS making up 83.5%. (ENISA ETL 2025) Finance also represents 11% of significant-impact incidents reported under NIS in 2024. (ENISA ETL 2025) The infrastructure implication is that even short downtime can have outsized societal and reputational effects.

Health is high-risk due to low downtime tolerance and platform dependence. A Romanian case illustrates how shared platforms amplify scope: reporting indicates 25 facilities had data encrypted and 75 additional hospitals using the platform were disconnected from the internet as a precaution. (The Record, 13 Feb 2024) The infrastructure mechanism is containment externalities: even entities not confirmed compromised can experience disruption due to defensive isolation of shared systems.

Energy/utilities and water carry high salience because incidents can produce direct service impacts. Associated Press reports a Denmark waterworks incident in which attackers changed pressure, contributing to a pipe burst; the result was measurable service impact: ~50 households without water for ~7 hours and ~450 houses without water for ~1 hour. (AP, 19 Dec 2025) Even when geographically limited, these incidents demonstrate proof-of-effect against essential services and generate disproportionate political and societal attention.

6. Modalities and Access Vectors

Fig. 2 - Distribution of incident types.
Source: ENISA dataset



The EU infrastructure threat environment is best represented as a two-lane pipeline: (A) high-volume availability disruption and (B) lower-volume intrusions that generate high-consequence outcomes (extortion, data theft, and persistence). ENISA shows DDoS dominates recorded cases (76.7%), while intrusions account for 17.8%. (ENISA ETL 2025) Availability pressure drives incident workload and public visibility; intrusions drive ransomware, data theft, and persistence.

For intrusions, initial access is dominated by phishing and exploitation. ENISA reports phishing accounts for about 60% of observed entry points, while exploitation of vulnerabilities accounts for 21.3%. (ENISA ETL 2025) Conversion is the operational distinction: ENISA reports 27% of phishing cases led to intrusions, while nearly 70% of vulnerability cases culminated in intrusions; 68% of vulnerability-based incidents resulted in deployment of malicious code. (ENISA ETL 2025) This supports a concrete prioritisation for infrastructure defence: reduce exposed edge services, shorten patch timelines, and harden identity and remote access, because exploitation converts to malware and disruption at higher rates than phishing alone.

Patch latency at the edge sustains scalable compromise. Verizon's DBIR executive summary reports edge devices/VPNs as a major exploitation surface (22% of vulnerability exploitation targets), with a median 32-day remediation time and only ~54% of those edge vulnerabilities fully remediated across the year. (Verizon DBIR 2025 Executive Summary) In infrastructure environments, patching is constrained by uptime requirements, vendor dependencies, and change-control processes; this creates predictable attacker advantage when vulnerabilities are weaponised rapidly.

Post-compromise outcomes in the EU incident set are heavily monetisation-oriented. ENISA reports that ransomware, banking trojans, and infostealers constitute 87.3% of malicious code deployed following recorded intrusions and that 68.6% of recorded intrusions led to data breaches leaked on cybercriminal forums for sale. (ENISA ETL 2025) This implies that "infrastructure intrusion" is frequently an access-and-data economy as much as an encryption economy.

Third-party compromise amplifies blast radius. ENISA reports supply chain risks as 10.6% of threat categories, signalling material exposure to indirect pathways through vendors and dependencies. (ENISA ETL 2025) The airport disruptions linked to a third-party provider illustrate this logic: compromise of one service node can create multi-entity and multi-country disruption without direct compromise of each endpoint. (Reuters, 22 Sep 2025)

Quantified impact is clearest in ransomware recovery burden. Sophos' 2024 critical infrastructure ransomware study (energy/oil-gas/utilities) reports 67% of organisations were hit by ransomware in 2024, attackers attempted to compromise backups in 98% of cases (succeeding 79% of the time), and the mean recovery cost was $3.12M. (Sophos CI Ransomware 2024) Ransomware clearly degrades restoration capacity, raises recovery costs, and increases downtime risk, especially where segmentation and backup integrity are weak.

7. Conclusion

The 2024–2025 evidence base supports a clear prioritisation for EU infrastructure cyber risk. Public administration and transport are the most consistently pressured targets for high-visibility availability disruption. High-consequence risk concentrates in the intrusion pipeline, credential abuse and vulnerability exploitation, amplified by patch latency at edge services and by third-party dependencies. The infrastructure most at risk is not only the most frequently targeted, but also the most dependency-entangled: public administration (visibility + strategic intrusion), transport/logistics (time sensitivity + vendor choke points), digital infrastructure/communications (systemic multiplier), finance (trust externalities), and energy/utilities and health (high recovery burden and low downtime tolerance).

References

- Burrows, E. (2025, December 19). Denmark blames Russia for cyberattacks on water utility that left houses without water. AP News. https://apnews.com/article/russia-denmark-cyberattacks-moscow-putin-sabotage-d9776a44bf6b80574eb54a5edf64ee19
- Computer Emergency Response Team for the EU Institutions. (2025, February 25). Threat landscape report 2024: A year in review. https://cert.europa.eu/publications/threat-intelligence/tlr2024/
- European Commission. (2022). NIS2 directive: Securing network and information systems. Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
- European Union Agency for Cybersecurity. (2024, September 19). ENISA threat landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

- European Union Agency for Cybersecurity. (2025, October 1). ENISA threat landscape 2025. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

- Europol. (2025, June 11). Steal, deal and repeat: How cybercriminals trade and exploit your data (Internet organised crime threat assessment [IOCTA] 2025). https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data

- Mahendru, P. (2024, July 17). The state of ransomware in critical infrastructure 2024. Sophos. https://www.sophos.com/en-us/blog/the-state-of-ransomware-in-critical-infrastructure-2024

- Microsoft. (2024). Microsoft digital defense report 2024. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024

- Reddick, J. (2024, February 13). Hospitals offline across Romania following ransomware attack on IT platform. The Record. https://therecord.media/romanian-hospitals-offline-after-ransomware-attack

- Reuters. (2025, September 22). EU agency confirms ransomware attack behind airport disruptions. Reuters. https://www.reuters.com/business/aerospace-defense/eu-agency-says-third-party-ransomware-behind-airport-disruptions-2025-09-22/

- Verizon. (2025, May 5). 2025 data breach investigations report: Executive summary. https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf