European
Repository of
Cyber Incidents

European Repository

# Cyber Conflict Briefing

# 2025 CYBER ACTIVITY BALANCE

## The European Union in Focus

Lena Rottinger
Annegret Bendiek
Jonas Hemmelskamp

UNIVERSITÄT HEIDELBERG ZUKUNFT SEIT 1386
SWP Stiftung Wissenschaft und Politik German Institute for International and Security Affairs
universität innsbruck
CPI CYBER POLICY INSTITUTE

## *About the authors*

**Lena Rottinger** is an academic researcher in the EuRepoC project and is responsible for the political coding of cyber incidents. Previously, she completed her Master's degree in Political Science at the University of Heidelberg and the University of Bologna with a focus on International Relations.

**Dr. Annegret Bendiek** is Co-Lead of the Cluster “Cybersecurity and Digital Policy” and Senior Fellow in the EU/Europe Research Division at the German Institute for International and Security Affairs (SWP Berlin). Annegret serves as one of the principal investigators of EuRepoC.

**Jonas Hemmelskamp** is Chief Data Scientist for the EuRepoC project and a PhD student at the Institute of Political Science at the University of Heidelberg. He completed his master’s degree in political science at Heidelberg University, where his thesis examined hybrid threat indicators.


linkedin/EuRepoC

contact@eurepoc.eu

https://eurepoc.eu

@eurepoc.bsky.social



**About this report**

The Cyber Conflict Briefing and Cyber Activity Balance are analytic products prepared by EuRepoC. The German edition is published in collaboration with **Tagesspiegel Background - Cybersecurity.**

This Working Paper was prepared as part of the 2026-27 Project “Europäische Diplomatie und Normbildung. Potentiale für eine operative Cyber-Incidents- und Responseforschung heben” which is funded by the German Federal Foreign Office.

*February 2026*

## Between Solidarity and Subsidiarity: The EU's Cybersecurity Balance in 2025

In January 2026, the European Commission introduced a comprehensive Cybersecurity Package comprising a revision of the Cybersecurity Act and targeted amendments to the NIS2 Directive. The draft cybersecurity package by the Commission aims to enhance cooperation between EU Member States, primarily by strengthening the operational mandate of ENISA. By actively participating in the CSIRT-Network and EU CyCLONe and jointly developing Repositories for Cyber Threat Intelligence with other authorities like Europol, ENISA is to become a hub for shared situational awareness.

The initiative rests on a central premise: that enhanced cooperation and improved information-sharing will enable the European Union to better detect, interpret, and respond to an evolving cyber threat landscape. Situational awareness has thus become both a diagnostic tool and an objective of EU cybersecurity governance. Yet situational awareness is only as robust as the assumptions underpinning it. The Commission's draft implicitly assumes that existing coordination gaps can be addressed primarily through enhanced operational mechanisms and that large-scale incidents represent the principal stress test for European solidarity.

The 2025 Cyber Balance evaluates these assumptions against empirical developments documented in the European Repository of Cyber Incidents (EuRepoC). EuRepoC has been tracking politically-relevant cyber operations and states' responses dating back two and a half decades. The Repository combines this depth in data with the continuous daily expansion of the dataset to enable short-term and long-term trend analysis. This Cyber Activity Balance draws on EuRepoC's open-source data to empirically assess the challenges the new regulatory package needs to address to achieve a future-proof European situational awareness.[1]

The EuRepoC findings highlight the problem of the cumulative effects of cyber attacks, which are not defined in more detail in the legal acts. While the overall number of unique operations targeting EU entities has slightly decreased, the number of affected targets has increased, indicating growing cumulative and spill-over effects across interconnected sectors. At the same time, individual operations often remained below the formal threshold of "large-scale" cyber incident, yet cumulatively contribute to systemic strain.

These trends raise a fundamental question: Does the draft regulation sufficiently account for the cumulative, transnational, and often sub-threshold character of contemporary cyber operations? Or does its reliance on subsidiarity-based activation mechanisms risk reinforcing fragmentation in precisely the areas where coordination is most needed?

Against this backdrop, the analysis contrasts regulatory ambition with empirical evidence. It assesses whether the architecture proposed by the Commission can strengthen European solidarity (Art. 2 TEU) in practice, or whether it leaves structural blind spots in the face of persistent, ambiguous, and strategically distributed cyber activity.

[1] Details on the methodology used for collecting the data are available at https://eurepoc.eu/methodology/

## Intensity and volume of cyber incidents against the EU/Europe in 2025

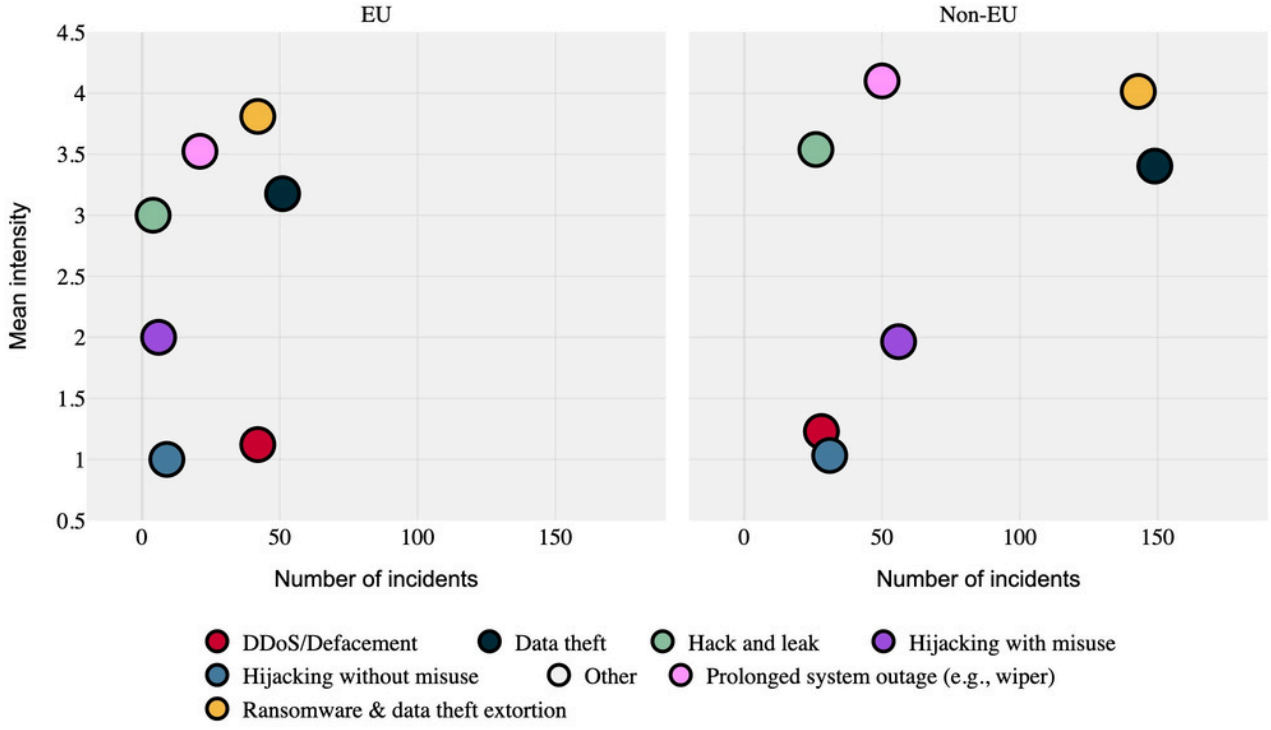
Since 2020, there has been a steady increase in cyber operations targeting EU entities. But in 2025, a slightly lower number of unique operations against EU targets included by EuRepoC went alongside an overall higher number of affected targets. It marks the first year since the COVID-19 pandemic in which EuRepoC tracked fewer operations than in the previous year, with 211 operations included in 2024 and 179 operations included in 2025. But in parallel, the number of EU targets affected by these operations has increased from 357 to 388. This observation supports the idea that single incidents are increasingly affecting multiple organisations at once and is in line with an increase in attacks targeting supply chains and digital providers described below.

Considering the slight decrease in the volume of operations tracked globally (excluding EU member states) of 17.67 percent (from 583 to 480) alongside a decrease of 21.15 percent in receivers (from 1045 to 824), this development points to a relative concentration of operations in EU member states.

At the same time, the operations in EU member states tracked for 2025 generally disrupted services for a slightly shorter period of time and stole data of slightly lower sensitivity than in the previous year. This is indicated by the average value of the intensity indicator dropping from 2.8 to 2.6. Among the 2025 operations, there were only 11 reaching the highest intensities of 5 and 6, whereas in 2024, there were 18 operations at this level.

This decrease in the intensity of individual operations does not signal a decrease in the systemic disruption attempted by cyber-

### Intensity and Volume of Cyber Incidents Targeting EU Member States and Third Countries in 2025




Source: EuRepoC Global Database as of 03.02.2026.

attacks. While the statistical intensity within EU borders decreased, this data excludes a severe kinetic incident in Norway. Additionally, a severe attack against the Polish energy grid was successfully thwarted before it could achieve systemic and statistical impact.

In fact, Russian state-aligned operations focus even more on disruptive actions than in previous years. Disruptive elements are now included in over 69 percent of operations attributed to actors of Russian origin (up from 55 percent) and continue to cause significant damage to the energy and transport sectors in Norway, France, and Poland. "Over the past year, we have seen a change in activity from pro-Russian cyber actors," Beate Gangås, head of Norway's PST security police agency, said in August 2025. The following attacks are particularly noteworthy regarding their intensity:

1. In April 2025, Russian-linked hackers temporarily seized operational control of a hydropower dam in western Norway, deliberately manipulating physical systems by opening floodgates and releasing large volumes of water over several hours before detection. Although no casualties occurred, the attack demonstrated a capacity to translate cyber intrusion into real-world kinetic effects, underscoring elevated operational sophistication and intent. Given Norway's heavy reliance on hydropower, the breach amplified systemic risk to national energy security.

2. In late December 2025, La Poste was hit by a large-scale distributed denial-of-service (DDoS) cyberattack that overwhelmed its online infrastructure with billions of malicious requests per second, rendering websites, parcel-tracking tools, and digital banking services intermittently inaccessible during the peak pre-Christmas period. The assault was unprecedented in intensity for this type of attack. This is supported by the observation that only a small number of attacks by NoName led to prolonged service outages. Although no data breach occurred, and core postal and banking systems remained secure, the sustained high-volume traffic caused significant disruption to customer access and service continuity.

3. On 14 January 2026, Poland's Prime Minister Donald Tusk informed government leaders about a cyberattack conducted on 29 December 2025 against national energy infrastructure. Although the attack was successfully thwarted and did not compromise system integrity, its threat level was unprecedented. It constituted the first large-scale, coordinated cyber operation targeting distributed energy resources across multiple sites simultaneously. Unlike prior incidents limited to single facilities, this attack demonstrated a high level of sophistication, coordination, and intent to disrupt critical operational technology.

Although these cyber incidents are significant, there is no evidence that they meet the threshold of "large-scale" incidents as defined by the NIS2 Directive. They did not simultaneously affect multiple EU Member States, nor did they overwhelm the response capacities of the states concerned. However, these events should not be regarded as isolated or exceptional occurrences. Rather, they constitute the most visible manifestations of a broader and sustained pattern of persistent, often ambiguous, cyber activities directed against the European Union.

In light of the four observations identified in the 2025 Balance, a more fundamental question emerges: at what point do the cumulative effects of recurrent cyber incidents trigger the EU solidarity clause

(Art. 222 TFEU)? In other words, even if individual incidents remain below the formal threshold of a "large-scale" attack, can their aggregated impact—over time and across sectors—create a situation that warrants collective European action?

## Four Observations on the EU Cyber Threat Landscape of 2025

### Observation 1: A Shift in the Type of Cyber Threat Activity

Compared to 2024, the overall number of cyberattacks targeting entities in critical infrastructure sectors across EU member states has, in fact, decreased from 115 incidents to 87 incidents in 2025. But alongside this overall decrease, the distribution of targeted sectors has shifted significantly over the past year.

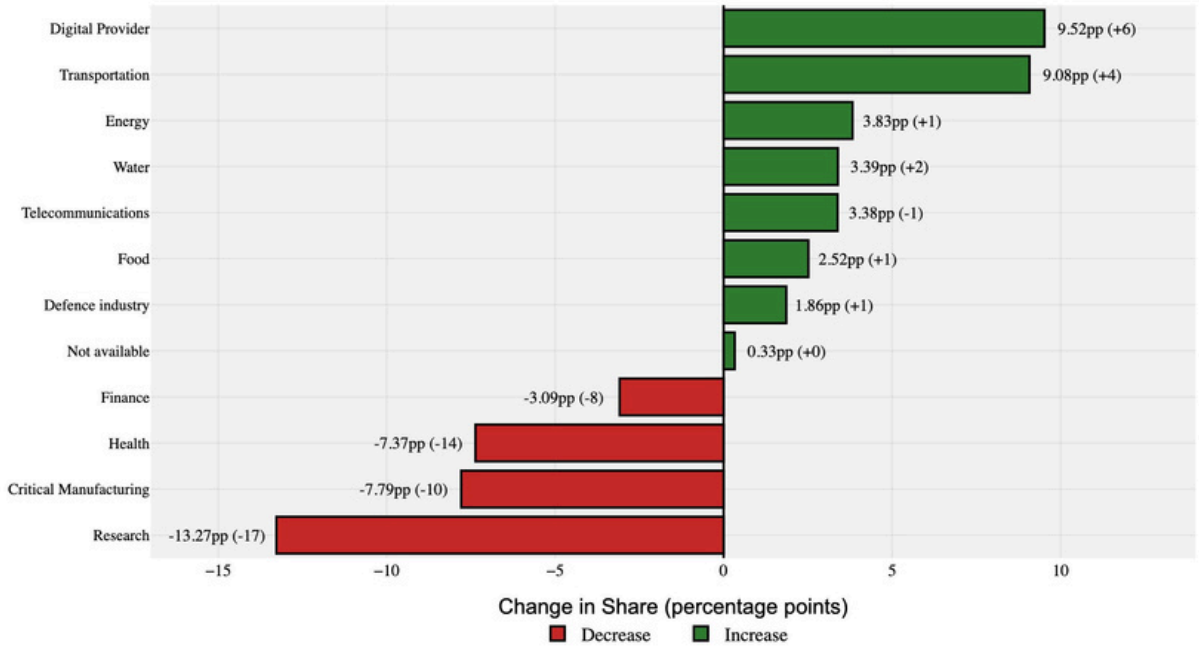
Historically, the health sector has been experiencing the largest volume of incidents among critical infrastructure sectors. The year 2024 reinforced this pattern and most of the tracked incidents targeted healthcare entities. In 2025, however, this long-term trend changed. The share of incidents targeting the health sector decreased by 7.37 percentage points, leaving it with 15 tracked incidents and positioning it as only the second-most targeted sector.

Instead, transportation emerged as the top targeted sector in 2025, with its share of incidents rising by 9.08 percent points. An even more pronounced increase was observed in attacks against digital providers, whose share increased by 9.52 percentage points year-on-year.

**a) Digital Providers**

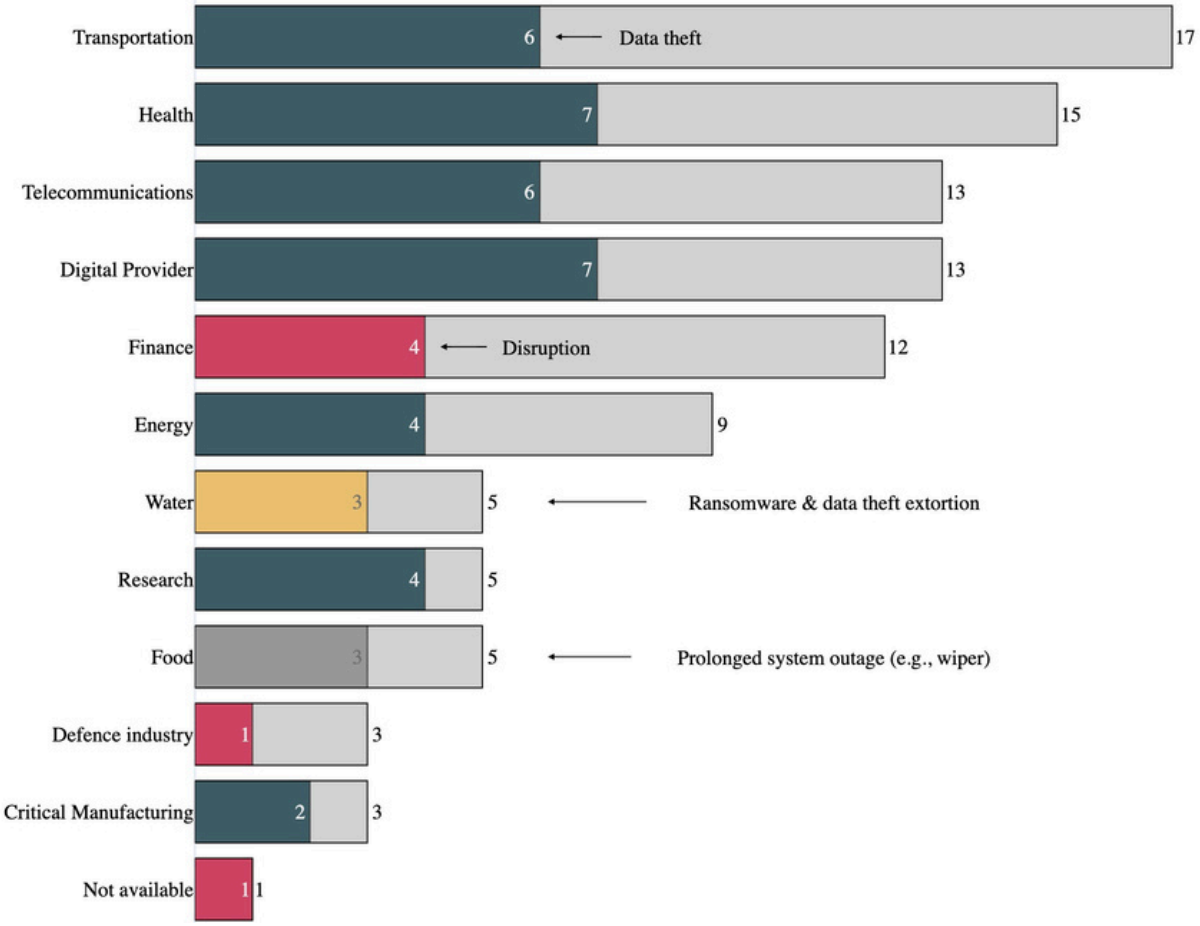
The rise in targeted digital providers coincides with the increasing focus of threat actors on exploiting digital dependencies and supply-chains as previously reported by ENISA (p. 11). While most of these incidents remain unattributed or are attributed to criminal collectives without clear country of

Change in Share of Cyber Incidents Affecting EU Member States Critical Infrastructure by Sector (2024 to 2025)




Source: EuRepoC Global Database as of 03.02.2026.

## Most Frequently Targeted Critical Infrastructure Sectors and Incident types in EU Member states in 2025




origin, attacks on digital providers allow the perpetrators to rapidly breach large numbers of interconnected organisations, often enabling them to steal the data of millions of people, and to disrupt services on an unprecedented scale across vast regions. This development goes alongside the overwhelming success these attacks recently had. One example is the misuse of the Salesloft Drift application and the subsequent extortion of major corporations worldwide.

After UNC6395 was able to misuse OAuth Tokens issued by the Salesloft Drift application over a longer period, their subsequent actions enabled them to breach dozens of major organizations, including FedEx, AirFrance and KLM, Marriot, Cisco, and Google Adsense. While the exact link between UNC6395 and Scattered Lapsus$ Hunters remains debated, these organisations have been extorted by the latter.

There have been two other particularly noteworthy attacks in the sector:
1. The most reported incident is the widespread disruption of at least seven major European Airports on 19 September after a breach of Collins Aerospace's Muse Software. The Repository is tracking 392 reports on this event. The company initially reported a "cyber-related disruption". It was later confirmed by ENISA that the event was a ransomware attack. Everest Ransomware claimed responsibility for the incident, stating they breached the provider on 10 September 2025 and obtained data of 1,5 million passengers. However, the group denied having deployed ransomware. Reporting by ENISA and NCSC-UK suggests a coinciding intrusion from a different threat actor is possible.

2. The second notable incident occurred on 23 August, when unattributed threat actors breached Miljödata, a data service and system provider for Swedish Municipalities. The fallout of this attack affected around 200 municipalities and regions across Sweden, as well as Volvo North America. The threat actors demanded a ransom of 1.5 bitcoins (which is approximately 135.000€). In mid-September, the data of 1.5 million Swedes obtained during the breach was leaked.

A large portion of the remaining incidents targeting Digital Providers specifically targeted companies that are providing digital services to the civil administration in municipalities across EU member states. Most of them remained unattributed as of February 2026.

**b) Transportation**

Out of 18 incidents targeting the transportation sector, 7 had disruptive elements. The sector is once again one of the preferred targets of the Russian state-aligned hacktivist collective NoName057(16), and while not all their attacks have been publicly attributed, the group claimed some of the unattributed ones, e.g., the attacks on German railway providers Hannover S-Bahn and Metronom on their telegram account.

2025 was also the year in which the German government officially attributed the intrusion of German Air Traffic Control (DSF), which already happened in August 2024, to the Russian state-sponsored group APT28/Fancy Bear. Media reports had already suggested the Russian responsibility shortly after the breach.

The remaining transport-sector incidents of 2025 showed patterns of either data theft or ransomware activity. Incidentally, the incident with the highest intensity in this sector was before-mentioned breach of Collins Aerospace, which subsequently affected the international airports employing the application. The scaled intensity of this incident was 2.7, whereas the average for the sector in 2025 was just 1.85. Other incidents in the transport sector, e.g., the breaches of KLM or AirFrance, are then again related to the fallout of the Salesloft Drift incident.

The relative increase in both sectors is, thus, interrelated because many of the incidents in the transport sector are related to attacks on third-party digital suppliers. This holds true for the breaches at the Berlin public transport company BVG in July or Royal Mail in March, which were both related to breaches of third parties. Taking a different perspective, Everest Ransomware allegedly claims they were not particularly targeting air traffic industry, but emphasised they were “doing security research” and were particularly concerned about security issues in an industry responsible for the security of vast amounts of travelers.

## Observation 2: Ransomware as a Transnational Threat

Ransomware and other criminal groups do not reinforce the pattern of most incidents being unattributed because they mostly self-attribute in the process of extorting their victims. Even though the Repository does not track these statements of the Ransomware groups on their leak sites themselves but relies on publicly disclosed incidents and attributions, 23 (56%) of the 41 tracked Ransomware attacks in EU member states have been attributed publicly to one of these groups.

A typical pattern these attacks do reinforce is that the attributions mostly do not include a country of origin. While the country of origin is known or suspected in the case of specific groups (e.g., because their malware does not target systems with Russian as the primary language), many of them are tracked with the country of origin being unknown. Besides the fact that they do not self-attribute the country of origin, one factor is also that these groups operate in a transnational fashion. This holds true for the individuals affiliated with the groups, their infrastructures, and their target selection.

**a) Transnational Target Selection**

In 2025, the 10 most active criminal groups breaching targets in EU member states have, on average, targeted organizations in 3.9 countries worldwide. This list is led by UNC6395 (11 countries) with the fallout from the previously mentioned Salesloft incident, Everest Ransomware Group (8 countries), and Warlock (countries across Europe and North as well as Latin America). The Salesloft incident further shows how digital provider platforms are ignoring borders, with the effects of just one breach being able to spill over to at least 11 countries.

These transnational aspects of cyber threats become even more pronounced when including state- and state-affiliated actors. The average then jumps to 12.2 targeted countries, led by North Korean state-sponsored group Lazarus (31 countries) as well as Chinese APT27 (Linen Typhoon, 13 countries) and APT31 (Violet Typhoon, 13 countries). This stands in stark contrast to the Russian groups active in EU member states. These groups rather focused on surgical disruptive strikes and targeted only 2.75 countries on average, and specifically focused on EU member states (e.g., Noname057(16)). These groups are also somewhat distinct from the Russian groups active in Ukraine, where i.e. Sandworm (who spilled over to Poland in December 2025) or Gamaredon, as well as multiple unclassified clusters, are particularly active.

**b) Transnational Infrastructures & Individuals**

There are clear transnational aspects to the ecosystem of cyber-criminal networks. The Criminal as-a-service (XaaS, i.e. Ransomware-as-a-Service) models spread across many countries and do not stop with Ransomware services. While Russia is offering a safe haven to cybercriminals, the infrastructures and reach of many criminals may be clustered in, but not limited to, Russia.

The extent of this transnational cyber-crime nature often becomes visible in response to these activities. In July 2025, the US Department of the Treasury sanctioned Aeza Group, a Russia-based bulletproof hosting service provider, for its role in supporting cybercriminal activities around the world. While most of the subsidiaries were Russa-based, Aeza International Ltd. was a UK-based front company which was used to lease IP addresses to cybercriminals, including, for example, Meduza inforstealer. Later sanctions also targeted another front company, Hypercore Ltd. (again registered in the UK), as well as a Serbian and an Uzbek company, both accused of attempting to evade sanctions.

The results of Operation Endgame further solidify this observation. The coordinated operation, first initiated in 2022 and including law enforcement from 11 states, initiated Phase 3 in November 2025. The action led to the search of 11 locations in Germany, Greece, and the Netherlands and took down 1025 servers worldwide.

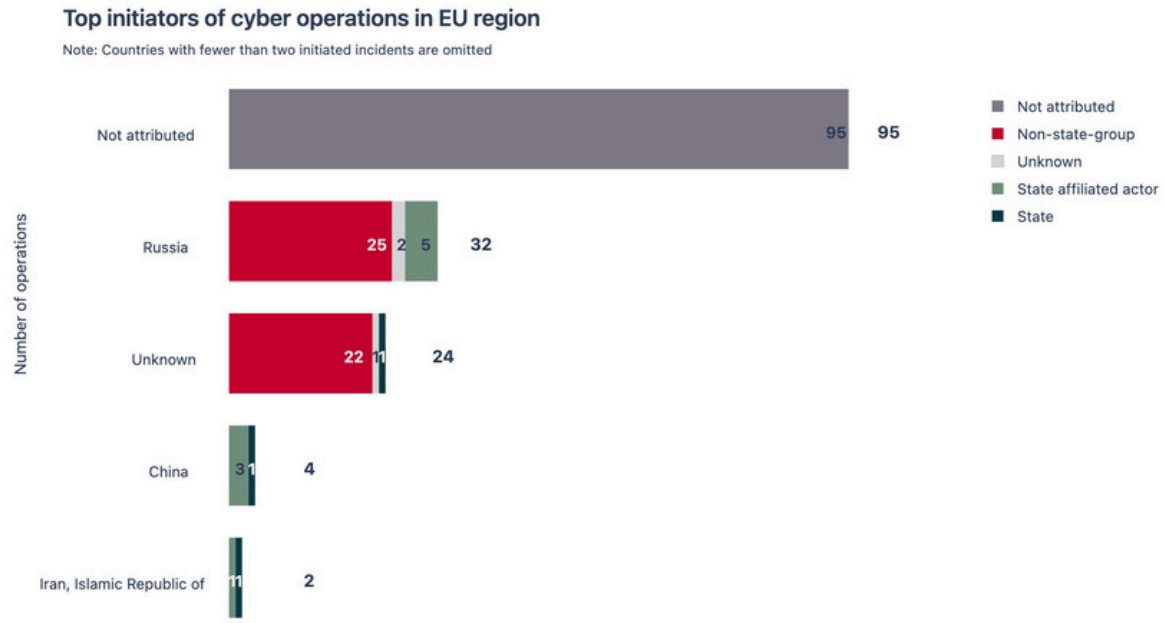
In December, the FBI and other U.S. agencies, the German BKA, and Finnish NBI took down a crypto-exchange called E-Note, which allegedly facilitated money laundering by transnational cyber-criminal organisations. According to reporting, the exchange was linked to criminals engaging in Ransomware attacks targeting U.S. healthcare and other critical infrastructures since 2017. And there are other criminal services across the world supporting the ecosystem as well. For example, law enforcement agencies from Estonia and Latvia, together with Europol and Eurojust, as well as cooperation with authorities from Austria, Estonia, and Finland, arrested seven criminals in October. The action dismantled a criminal network that offered SIM-box devices and rented telephone numbers from over 80 countries, facilitating phishing, smishing, and fraud.
Ransomware groups, therefore, operate both from and against several countries at the same time, relying on a growing ecosystem of criminal services. Successful operations by law enforcement have been increasingly international in nature, which further indicates that Ransomware is a transnational threat that must be combated internationally.

### Observation 3: A Growing Use of Proxy Actors

In 2025, EU Member States have been targeted mostly by Russia- and China-linked threat actors. Consistent with the pattern observed in 2024, Russian state-sponsored and affiliated threat actors prioritised disruptive cyber activity such as low-cost-high-visibility DDoS attacks as well as prolonged system disruptions at critical infrastructure entities.

Despite the apparent dominance of Russian non-state groups, particularly self-proclaimed hacktivists, developments in 2025 suggest that the boundary between state-directed operations and ostensibly independent hacktivist campaigns is no less permeable than in other forms of Russian proxy activity.

## Top Initiators of Cyber Operations targeting EU Member States in 2025




Source: EuRepoC Global Database as of 03.02.2026.

The activities by and against two of these groups are particularly notable: (1) The most active threat actor in Europe was Russia-linked NoName057(16), according to EuRepoC data. NoName057(16) emerged in March 2022 and was mostly considered a pro-Russian hacktivist group active since Russia's full-scale invasion of Ukraine. The group has been notorious for its large-scale DDoS campaigns through its mostly volunteer-driven "DDoSia" platform. A successor to the Bobik botnet, DDoSia encompasses the entire ecosystem of tools, infrastructure, and volunteers necessary to run this long-term DDoS campaign. Another notable Russian group, Z-Pentest, breached Lake Risevat Dam Systems in Norway in April 2025 and managed to open its water valve at full capacity for hours before the intrusion was detected.

Throughout 2025, new information about both groups became public, providing striking details of how these groups operate. While threat intelligence analysis and political responses from 2022 and 2023 suggested the group was "merely" a hacktivist group, new evidence from 2025 links the group directly to the Russian state.

Between 14 and 17 July 2025, an international law enforcement operation code-named "Eastwood" was launched against NoName057(16)'s members and infrastructure. Led by Europol and Eurojust, Operation Eastwood involved simultaneous actions by law enforcement authorities in eleven European countries and the United States. The operation led to significant damage to NoName057(16)'s digital infrastructure and to the arrest of two individuals in France and Spain, as well as seven arrest warrants. Although the group went silent immediately after Operation Eastwood, the group resurfaced on 23 July with a Telegram statement and an increase in activity, including a change of strategy with a stronger focus on critical infrastructure systems. After the legal responses had only very limited success, political reactions at the international level became more frequent.

On 9 December, then, the United States and a broad coalition of global partners, including at least nine EU member states as well as Europol and Eurojust, released a joint advisory on the activities on pro-russian hacktivists. In the advisory, the authoring organizations directly linked the Russian "hacktivist" group CARR to military unit 74455 (Sandworm/APT44, the group that was also behind the 2015 power outtage in Ukraine and the attempted power outtage of December 2025 in Poland) of the Russian GRU and declared that the Z-Pentest group was founded in September 2024 by CARR members after they became dissatisfied with the level of funding provided by the GRU.

In the same advisory, NoName057(16) was assessed to have been established by the Russian Center for the Study and Network Monitoring of the Youth Environment (CISM), an entity established on behalf of the Kremlin. The advisory specified a direct linkage between employees of CISM with the development of DDoSia, the funding of network infrastructure for the group, as well as the administration of their social media channels, and notably the selection of targets.

## China

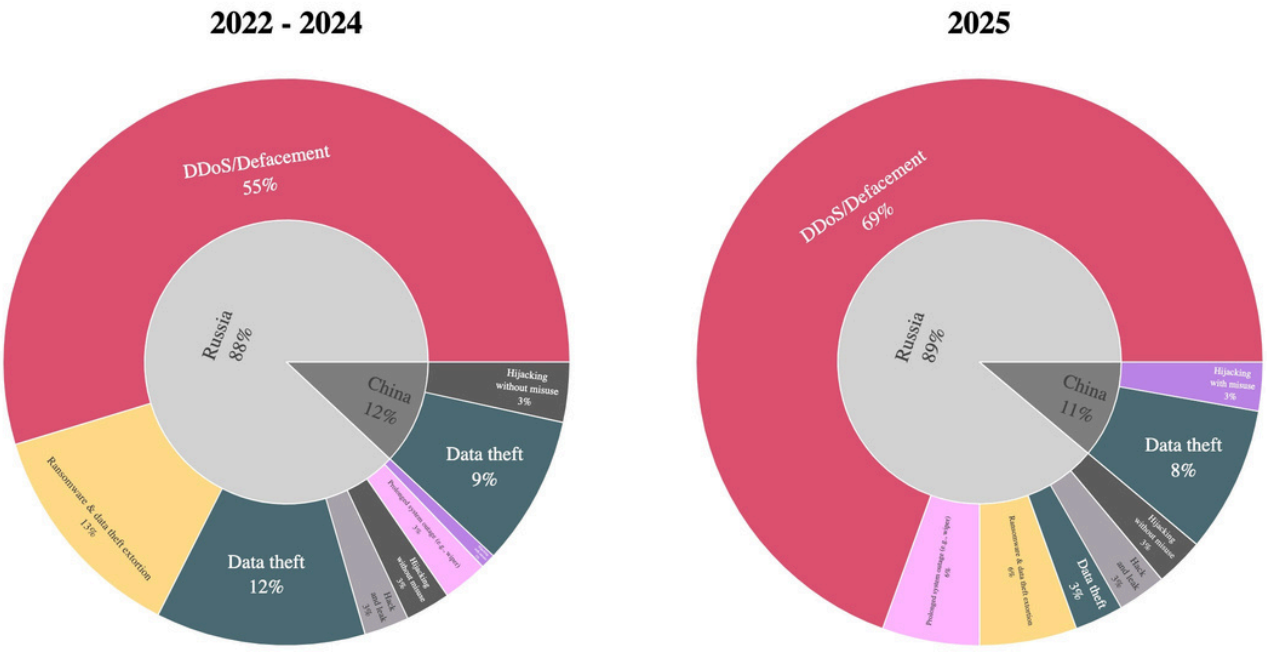
The Russian case remains a prime example of how the ambiguity of the state-non-state nexus complicates the attribution of direct or indirect state responsibility. While Russian cyber actors are loud, Chinese state-nexus actors tend to a more covert approach.

One reason why the number of incidents with attributed Chinese origin is comparatively low is that reporting often rests on a wider description of campaigns targeting many entities by abusing specific CVEs like ToolShell targeting SharePoint servers or specific firewall products affecting very large numbers of organisations across Asia, Europe, Latin-America and North-America. Because of this, EuRepoC can only track the complete operation with abstract sectoral receivers instead of specific ones.

In addition, Chinese actors show different operational patterns than Russian actors, focusing on espionage and hijacking without misuse (possibly related to prepositioning).

Making their attribution even harder, analysis suggests that Chinese state-nexus actors are beginning to use Ransomware not only for moonlighting, but also possibly as a smokescreen and/or exit option. This is underlined by the abuse of CVE-2025-53770 and CVE-2025-53771 before their disclosure exclusively by Chinese state-nexus actors APT27, APT31, and the Warlock Ransomware Group, which emerged in 2025. Because of their professionalism, threat analysts believe the latter to be tied to state-nexus actors. Thus, the real number of receivers of Chinese malicious activity is probably strongly masked because of missing disclosures and attributions. That said, with only 4 out of 34 attributed Chinese operations in 2025 targeting EU member states, it remains possible that China is showing restraint in targeting the EU.

### Incidents with Russian and Chinese origin targeting EU member states over time




Source: EuRepoC Global Database as of 03.02.2026.

## Observation 4: The Exploitation of Weaknesses in European Coordination

Considering the transnationality of cyber threats and the difficulty in attribution, it is striking that there is almost zero transparent multilateral coordination in attribution processes for specific incidents. The Repository defines a joint attribution as an attribution statement in which multiple countries make a joint assessment. This contrasts with incidents that have been attributed by multiple countries independently.

In 2025, the Repository did not track a single joint attribution for specific incidents targeting EU member states. For incidents targeting other states, there were 5 such attributions in comparison, and EU member states participated in 2 of them alongside the Five Eyes: In one instance, attributing APT28 for attacks against the United Kingdom, and in another instance, attributing the deployment of spyware against Uyghur, Tibetan, and Taiwanese groups to Chinese state-nexus actors.

While 9 EU member states did participate in establishing the link of NoName057 and CARR with the Russian state, Denmark didn't participate in the advisory from 9 December and instead unilaterally attributed several attacks against Danish organisations to both groups just 9 days later, on 18 December. This could be read as a fragmentation of European signaling strategies and possibly indicates a lack of structured processes and data siloization among the participating states.

The lack of European cooperation in cyber incident response is generally in line with previous observations by the Repository, which already analyzed measures applied based on the Cyber Diplomacy Toolbox and only found a very small number of restrictive measures (sanctions). When it comes to other responses, the most active EU member state was Germany, with 17 tracked political responses in 2025, followed by France (9), Italy (8), and Poland (6). Yet there was only a single incident triggering a political response by more than one EU member state, when the Council of the EU, alongside NATO and Czechia responded to the breach of a network at the Czech Foreign Affairs Ministry from 2022 on 28 May 2025. Notably, while EU member states did participate in the joint advisory on CARR and Z-Pentest in December, there have been no specific solidarity statements or joint actions by European states on the specific incidents targeting the Lake Risevatnet Dam in Norway or a waterworks facility in Denmark, and instead, the affected states acted unilaterally in response to their respective incidents.

Given that official attributions are a national prerogative, the lack of joint attributions is not surprising, but still concerning. Coordinated EU responses, i.e., in the form of declarations by the High Representative on behalf of the EU, remain scarce. Apart from the above-mentioned solidarity statement by the EU concerning the Chinese cyber operation targeting the Czech Foreign Ministry, the EU only issued a second statement condemning Russia's persistent hybrid campaigns against the EU. In this statement, the EU endorsed several previous attributions by member states (e.g., the German and Czech attribution in 2024, and the French attribution in April 2025) and the new UK sanctions in response to GRU-led cyber operations. Even if the statement can be understood as an attempt to present a united European front, it reveals more fragmentation than cooperation.

## Consequences for the EU's Solidarity Clause (Art. 222 TFEU)

The four observations discussed above are likely to shape the effectiveness of the proposed Cybersecurity Package. Under the draft framework, ENISA's future mandate is closely connected to the coordination mechanisms established by the Cyber Solidarity Act (CSA). In accordance with the principle of subsidiarity, these mechanisms are primarily activated in response to "large-scale cyber incidents," as defined in the NIS2 Directive—namely incidents that exceed a Member State's response capacity or significantly affect at least two Member States. This threshold-based design confines EU-level solidarity to situations of exceptional severity. At the same time, ENISA is tasked with implementing Repositories of Cyber Threat Information while respecting existing repositories within EU institutions and the Member States.

However, the empirical data—particularly from EuRepoC—suggest a more complex strategic environment. European cybersecurity policy increasingly emphasises situational awareness, reflecting the growing need to detect and interpret persistent patterns of hostile cyber activity. The threat landscape confronting EU Member States is characterised less by singular, overwhelming attacks than by sustained, strategically calibrated operations, notably those attributed to Russian state-nexus actors. The targeting patterns observed in 2025, including the heightened impact on the European transport sector, illustrate a deliberate and adaptive approach rather than sporadic disruption.

This development raises a structural question regarding the adequacy of the current activation thresholds. Russian cyber operations frequently remain below the threshold of armed conflict and are often designed to be legally and politically ambiguous. Individually, such incidents may not meet the CSA's "large-scale" criteria. Yet their cumulative effect—across sectors, over time, and throughout the Union—can erode resilience, strain administrative capacities, and undermine the functioning of the internal market. The strategic reality, therefore, is one of incremental pressure rather than isolated crisis.

In this context, the solidarity clause under Article 222 TFEU warrants renewed consideration. While traditionally associated with singular, grave emergencies, its logic is premised on collective response to threats affecting the Union as a whole. If persistent and coordinated cyber operations produce systemic and cross-border effects, even without triggering the formal NIS2 threshold in any single instance, the aggregated impact may nonetheless justify collective action grounded in solidarity. A strictly incident-based interpretation risks overlooking the structural consequences of prolonged below-threshold activity.

Against the backdrop of an increasingly transnational and ambiguous cyber threat environment, the rise in unattributed incidents further complicates this assessment. European cooperation on attribution remains comparatively cautious, even as strategic competitors conduct sustained operations against critical infrastructures. This asymmetry underscores the need to reconsider whether the EU's current coordination and solidarity mechanisms sufficiently capture the cumulative dynamics of contemporary cyber competition.

A more flexible interpretation—one that accounts not only for the scale of individual incidents but also for their aggregated strategic impact—may be necessary to ensure that Article 222 TFEU remains responsive to the evolving nature of cyber threats.

## *About EuRepoC*

The European Repository of Cyber Incidents (EuRepoC) is a European research project with the aim of making information and knowledge about cyber conflicts visible. It is led by the University of Heidelberg, in cooperation with the University of Innsbruck, the Stiftung Wissenschaft und Politik and the Cyber Policy Institute (Estonia). It is currently funded by the German Federal Foreign Office and the Allianz SE.

EuRepoC provides updates on new entries in the Repository in a daily curated cyber incident tracker, which is openly available for subscription.

**Eu**ropean
**Repo**sitory of
**C**yber Incidents

www.eurepoc.eu

UNIVERSITÄT HEIDELBERG ZUKUNFT SEIT 1386

SWP Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

universität innsbruck

CPI CYBER POLICY INSTITUTE