European
Repository of
Cyber Incidents

EuRepoC Cyber Conflict Briefing

Q4 2025

Kerstin Zettl-Schabath
Jonas Hemmelskamp
Lena Rottinger

Overall observations

In the fourth quarter (Q4) of 2025, a total of **207 new cyber operations** were added to the EuRepoC database, representing approximately 9.2 percent fewer operations than in the third quarter (Q3). Despite this slight decline, the figure remains well above the quarterly values recorded in the second half of 2024 and the first half of 2025, and exceeds the long-term quarterly average recorded by EuRepoC of 186 operations by 21 incidents.

The **average intensity** of the operations recorded during the quarter was 3.13, thus remaining above the historical average (2.94), while being slightly below the relatively high intensity observed in Q3 (3.24). In the short-term trend, the average intensity of recorded incidents has therefore declined somewhat.

About the briefing

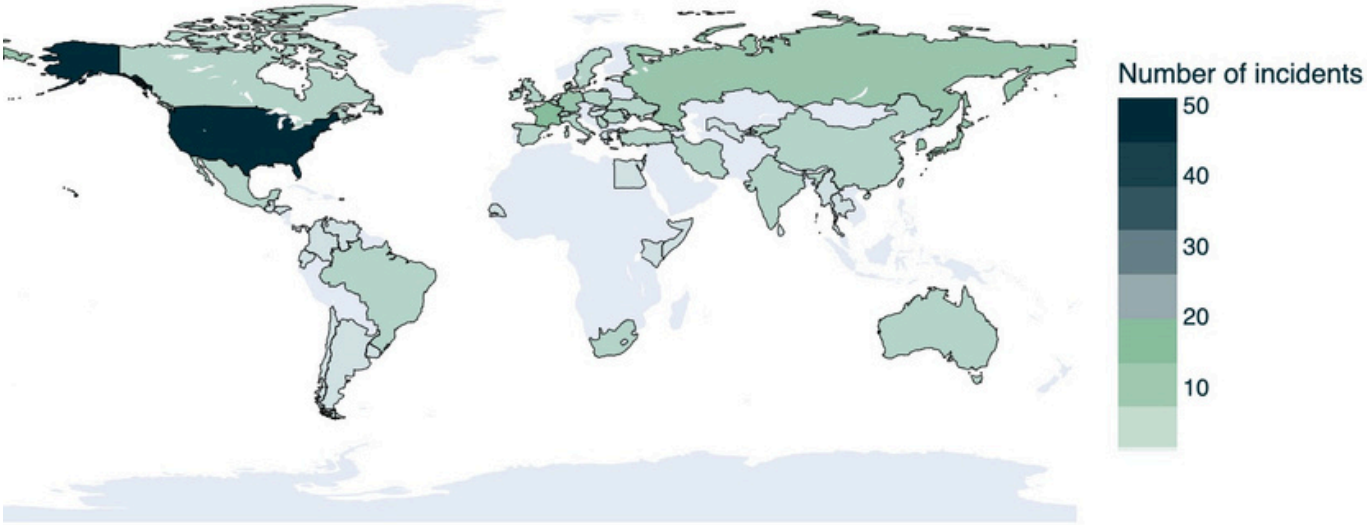
The Cyber Conflict Briefing is an analytic product prepared by EuRepoC. The German edition is published in collaboration with the **Tagesspiegel Cybersecurity Background,** accessible here.
It summarises the key trends, dynamics, and findings on cyber incidents as recorded by EuRepoC in a given month. These do not necessarily have to have taken place in Q4 2025, but may have started earlier. The focus is on technical, political, and legal aspects.

About EuRepoC

The European Repository of Cyber Incidents 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 Danish Ministry of Foreign Affairs.

Find out more at https://eurepoc.eu

Geographic distribution of operations in Q4 2025



Regional Trends

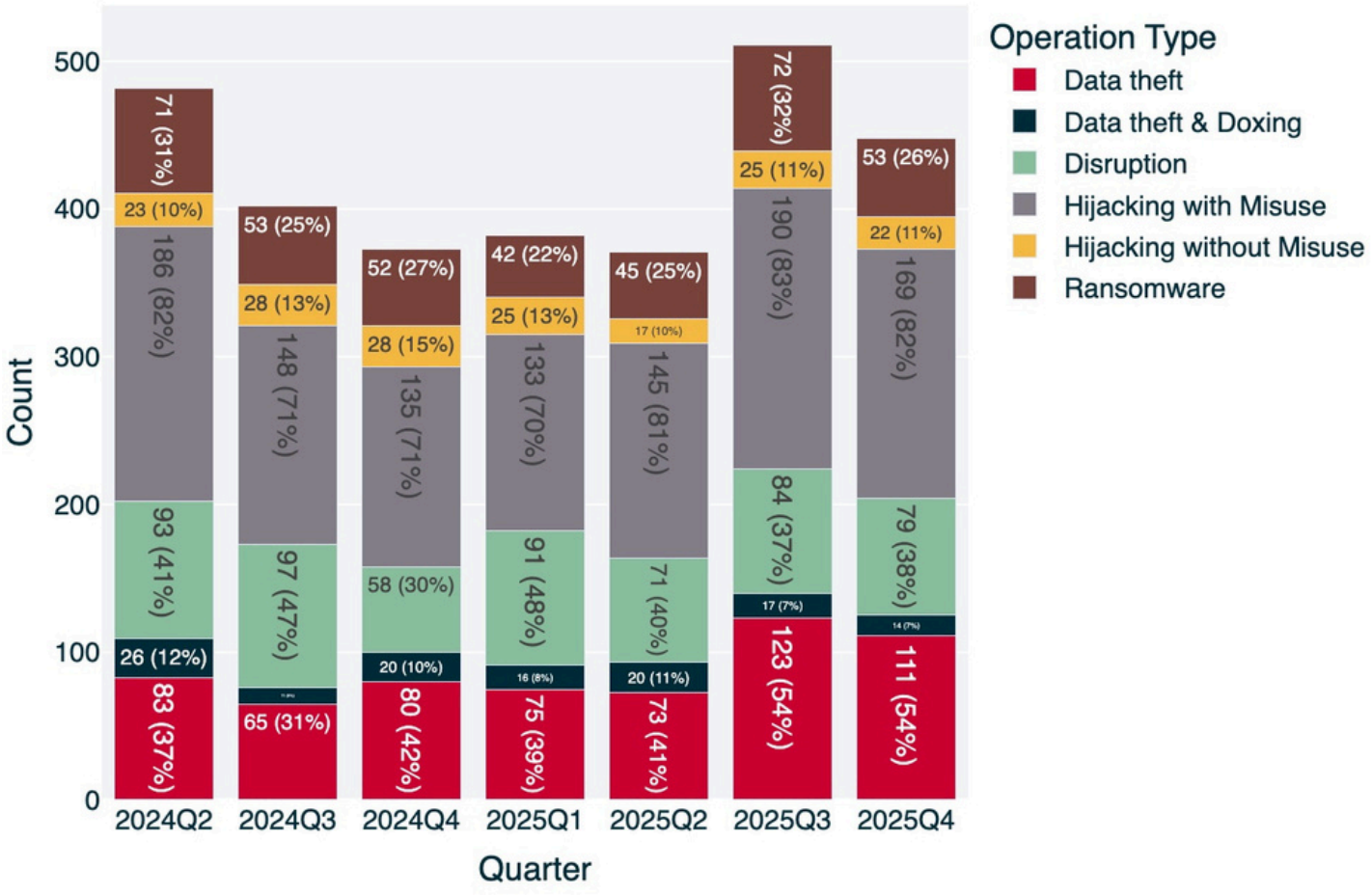
With 51 operations, the United States was once again the most frequently affected country this quarter. However, when considered in aggregate, the 27 EU member states, with 59 incidents, were targeted even more frequently than the United States. This represents the highest quarterly figure for EU member states since the last peak in Q2 2024 (61). Comparatively higher numbers of new operations targeting EU member states were recorded, particularly in November (25) and December (29).

At the national level, the United States was followed in Q4 by France (15), Germany (11), and South Korea (9). In France alone, ten new operations were recorded since early December, with the double attack on La Poste by NoName057(16) between December and January likely generating the greatest impact.

A similarly strong impact was observed in South Korea following the hack of Korea Telecom (KT) in August. As a result, an unusually high number of incidents affecting critical infrastructure were recorded in Q4. In several of these operations, North Korean actors such as the Lazarus Group are suspected.

The cybersecurity company Bitdefender also identified an unusual increase in ransomware activity in South Korea since September 2025, which it attributed to the so-called "Korean Leaks" campaign involving Qilin ransomware. There is suspicion that the North Korean state-linked group Moonstone Sleet, acting in an affiliate role, is using the services of the ransomware-as-a-service (RaaS) provider Qilin, further blurring the line between criminal and state-affiliated activities.

Distribution of Operation Types



Note: Individual cyber incidents may have several operation types in combination

The relative distribution of operation types remained consistent compared to the third quarter. The largest share of recorded operations, with 169 cases (82 percent), fell into the category “Hijacking with Misuse.” This category is usually coded in combination with others, such as disruption or espionage.

In the 12 cases in which "Hijacking with Misuse” appeared alone, attackers in Q4 pursued one of two objectives: data theft or defacement.

Cryptocurrency Theft and Defacement

Organizations specializing in cryptocurrency trading and decentralized finance (DeFi) protocols are particularly attractive targets for defacement and crypto theft. Beginning in August, a vulnerability in the BetterBank DeFi protocol was exploited to steal assets worth $5 million. In November, a security flaw in the DeFi protocol of the Balancer trading platform was deliberately exploited to siphon more than $100 million from smart contracts.

In late November, additional assets worth €33 million were lost in a hack of the South Korean cryptocurrency exchange Upbit. According to South Korean media reports, government officials once again suspect the Lazarus Group to be behind the incident. This would already be the second successful Lazarus attack on Upbit, following a similar hack in 2019.

Investigators also suspect North Korean actors in connection with a September incident involving the Japanese crypto miner SBI. Attacks on such organizations continue to serve as a source of funding for the North Korean state.

Website defacement also falls under "Hijacking with Misuse." In October, for example, the websites of four airports in the United States and Canada were compromised and modified with messages supporting Hamas and containing insults against Donald Trump and Benjamin Netanyahu. In November, several government websites in Kenya were taken over and defaced with white supremacist messages.

Espionage
The second most frequent type of operation consisted of data theft operations (54 percent). The repository recorded 111 operations of this type. These include ransomware attacks using so-called double extortion strategies, in which data is not only encrypted but also stolen, as well as attacks aimed specifically at data exfiltration.

In Q4, a significant number of espionage operations and long-term espionage campaigns conducted by Chinese actors were added to the EuRepoC database. Sixteen espionage operations were attributed to Chinese actors, compared with four attributed to Russia. These figures must, however, be contrasted with 39 unattributed pure espionage operations during the quarter.

As in Q3, the long-term Chinese espionage campaigns targeted a wide range of geographical areas, with a strong focus on Asian countries. At the same time, MustangPanda targeted European diplomats, while PhantomTaurus targeted embassies in the Middle East, Africa, and Asia. Campaigns by JewelBug and Salt Typhoon were discovered in Latin America, and the Ministry of State Security (MSS)-linked group APT31 has been conducting espionage in Russia's technology sector since at least 2022.

Chinese actors continue to focus particularly on telecommunications providers such as F5 and LG Uplus, as well as on digital solutions from Citrix and Cisco, and specifically on many attacks against Exchange servers worldwide. A frequently used attack vector remains the exploitation of the N-day vulnerability ToolShell.

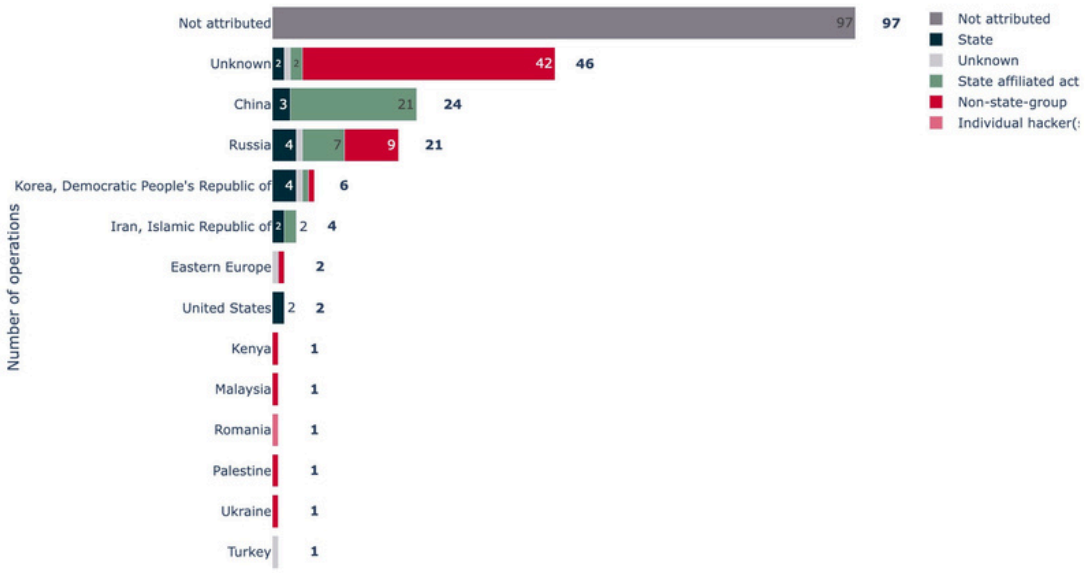
The relative share of politically relevant ransomware operations declined slightly, from the unusually high level of 32 percent in Q3 to a more typical 26 percent in Q4.

Threat actor profiles and attributions

In Q4, 47 percent of known incidents remained unattributed. Twenty-eight percent were attributed to non-state or individual hacker groups, 15 percent to state-affiliated actors, and 8 percent to state threat actors. China, Russia, North Korea, and Iran led the list of countries from which cyber operations originated.

Almost a quarter of all cyber incidents in the quarter were attributed to Chinese threat actors, most of whom were classified as state-supported or state actors. Media reports suggest that state-affiliated Chinese actors were behind the large-scale hack of the US network equipment provider F5. The same applies to the attack on the US Congressional Budget Office during the

Suspected countries of origin of initiators in Q4 2025



shutdown, the widely reported AI-based campaign by the Chinese group GTG-1002 against 30 critical infrastructure entities worldwide, and the incident at the UK Foreign Office attributed to STORM-1849.

A notable pattern is evident in who uncovered and attributed most Chinese attacks: in Q4, more than 80 percent were identified by private IT companies. Political reactions to Chinese cyber incidents were largely absent. Only the UK government imposed sanctions on 9 December 2025, against two Chinese companies (i-Soon and Integrity Tech) for their "reckless and irresponsible cyber activities."

Particularly noteworthy was the silence of US President Donald Trump despite repeated Chinese attacks on US institutions and critical infrastructure operators. This silence not only risks being interpreted as weakness but also normalizes China's deliberately harmful behaviour in cyberspace. At the same time, the lack of political response must be understood in the context of the six-week government shutdown in autumn 2025, which severely restricted the work of many US agencies.

Russian Threat Actors

A markedly different picture emerged in the case of Russian threat actors, who were held responsible for 21 cyber incidents in Q4. Several Western governments publicly commented on Russian cyber activities.

On December 9, 2025, the US Department of Justice announced legal action against two "state-supported cybercriminal hacker groups," namely CyberArmyofRussia_Reborn (CARR/Z-Pentest) and NoName057(16). Two indictments accused Ukrainian national Victoria Eduardovna Dubravna of conducting cyber operations against critical infrastructure in line with Russia's geopolitical interests.

The indictments distinguished between "Russian government backed" activity in the case of CARR and "state-sanctioned" activity in the case of NoName057(16). This represented the first politically significant statement establishing a direct link between NoName057(16) and the Russian state.

According to the indictments, NoName057(16) was a covert project involving several employees of the Center for the Study and Monitoring of the Youth Environment (CISM), which was established in 2018 by order of the Russian president. While NoName057(16) had previously focused primarily on DDoS attacks against political institutions, CARR/Z-Pentest became widely known following its attack on a Norwegian dam in April 2025.

In addition, CISA published a Joint Advisory together with thirteen allied states following Operation Eastwood in July. The advisory assessed the attacks by CARR and NoName057(16) as "less complex and with lower impact" than those conducted by advanced persistent threat (APT) groups. In Q4, Denmark was particularly affected by NoName057(16) attacks, especially in the context of municipal elections in November 2025. Danish authorities did not join the Joint Advisory but instead issued an independent statement attributing responsibility to Russia and summoned the Russian ambassador.

The German federal government also commented on Russian cyberattacks. Unlike Denmark's prompt response, German authorities reacted only one and a half years after the incident. On 12 December 2025, the federal government officially attributed the August 2024 attack on Deutsche Flugsicherung (Air Traffic Control) to the Russian hacker group APT28, also known as "Fancy Bear." According to the Federal Foreign Office, intelligence assessments demonstrate a direct link between the group and Russia's military intelligence service (GRU).

Developments in the Cybercrime Ecosystem

In Q4, numerous trends in the cybercrime ecosystem continued, while new developments emerged that may shape 2026. The hacker collective Scattered LAPSUS$ Hunters, composed mainly of adolescents, had attracted attention in previous months through numerous attacks on large companies, particularly in the UK. In Q4, reports again emerged of adolescents involved in criminal activities: in London, two teenagers were arrested for hacking and extorting a daycare center.

Scattered LAPSUS$ Hunters themselves acted even more confrontationally, reportedly publishing information about US government officials after Mexican cartels had allegedly offered bounties for such data. Whether increased law enforcement pressure on these young perpetrators—who, unlike most established ransomware groups, are based in Europe or the United States—will lead to less risky behaviour remains to be seen.

Another e-crime phenomenon that has received little attention in Europe but is being strongly combated internationally, especially by the US and China, is large-scale scamming operations originating in Southeast Asia, including so-called "pig butchering" schemes. In Q4, numerous sanctions, indictments, and convictions were imposed against key groups such as the Prince Group and its CEO. The US government established a dedicated task force, highlighting the priorities of the Trump administration following the dissolution of anti-disinformation units in 2025.

Reliable figures on German or European victims remain difficult to obtain, as the dark figure is often even higher than in ransomware cases.

Ransomware Trends

According to the platform ransomware.live, the number of recorded victims increased significantly again in November and December 2025. Qilin continued to establish itself as the most active ransomware-as-a-service (RaaS) provider and is likely based in the Russian region.

While law enforcement continues to focus on a few major groups responsible for most activities, it remains to be seen whether increasing fragmentation will undermine the effectiveness of these measures. Analysts report the emergence of "one-man" RaaS operations that develop and market their own ransomware variants with little effort.

Qilin was also a customer of BearHost, a major Russian bulletproof hosting provider that ceased operations in late 2025 "for political reasons," without compensating customers or granting access to their servers. Data center services operating from Germany have recently been linked by the Insikt Group to these "high-risk hosting networks," which are accused of hosting malicious infrastructure.

Further developments in the ransomware sector include:

- **Increasing abuse of legitimate tools:** Open-source DFIR tools such as Velociraptor, Nezha RMM, and TruffleHog, as well as platforms such as Dropbox and OneDrive and AI-based productivity tools, are being abused to evade detection and exfiltrate data.
- **Improved encryption:** The RansomHouse group now uses two keys per file (primary and secondary), making decryption significantly more difficult.
- **VPNs as primary access vectors:** According to At-Bay, VPNs have become the main entry point for ransomware over the past five years, while RDP usage has declined. Cisco and Citrix VPNs are particularly vulnerable.
- **Continued role of infostealers and initial access brokers:** These actors continue to drive ransomware activity. International operations such as the latest iteration of "Operation Endgame" achieved temporary successes against actors such as LummaStealer, DanaBot, and Rhadamanthys but failed to achieve lasting impact, as some groups quickly returned in new versions. However, easily exploitable targets remain, such as unchanged servers operated by the MedusaLocker ransomware gang, as criminals often improve their operational security only after incidents.
- **Shifted cost–benefit logic surrounding the acquisition and use of zero-day exploits:** Whereas these were previously largely reserved for long-term espionage operations by state actors, an increasing number of ransomware gangs now use them, sometimes "only" for data theft, but often also to extort customers of compromised software vendors.

Insider Threats

There has also been an increase in reports of cybersecurity incidents caused or facilitated by insiders or by individuals formally responsible for cybersecurity. Two US cybersecurity experts pleaded guilty to deploying ransomware against companies. In another case, CrowdStrike dismissed an employee who had passed information to Scattered LAPSUS$ Hunters.

In Q4, retaliatory attacks by dismissed employees against their former employers continued, often exploiting still-active account access. In 2026, insider threats are

likely to remain relevant, not least due to ongoing economic challenges in Germany and Europe, which may increase incentives for (former) employees.

Due to increased staff turnover, spearphishing campaigns targeting recruitment and hiring processes are also expected to continue. Both non-state and state-affiliated actors may be involved, including those from North Korea, Iran, and Vietnam. The North Korean regime reportedly generated more than $2 billion in 2025 alone through ransomware, crypto theft, and the infiltration of companies using fake remote employees. Cybercrime therefore remains an attractive financing tool for states despite sanctions.

More from EuRepoC

EuRepoC informs about new cyber incidents added to the database with a Cyber Incident Tracker, updated daily. You can subscribe here.

About the authors

Kerstin Zettl-Schabath is a Senior Cyber Threat Intelligence Analyst at the German Cyber Security Organisation (DCSO).

Jonas Hemmelskamp is the Chief Data Scientist at the European Repository of Cyber Incidents and is a doctoral candidate at the Institute for Political Science in the University of Heidelberg.

Lena Rottinger is a master's graduate of the University of Heidelberg and is an academic researcher with EuRepoC; she is responsible for the political coding of cyber incidents.

Follow us on social media

@EuRepoC

linkedin/EuRepoC

contact@eurepoc.eu

https://eurepoc.eu