European
Repository of
Cyber Incidents

EuRepoC Cyber Conflict Briefing

February 2024

Jakob Bund
Kerstin Zettl-Schabath
Martin Müller
Camille Borrett (Data Support)

Overall observations

In **February 2024**, EuRepoC recorded 107 cyber operations, marking a 24.4% surge compared to the previous month. This figure surpassed the overall average in recorded activity of 71 cyber operations per month by 36.

The **average intensity** of operations recorded in February 2024 registered at 3.25, exceeding the historical average (2.79). The notable uptick in operations since February 2023 is partly attributed to an expansion in EuRepoC's inclusion criteria. As of March 2023, EuRepoC has systematically been recording operations conducted against critical infrastructure targets and no longer makes inclusion contingent on whether these activities are linked to political or governmental threat actors or victims.

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 February, but may have started earlier. The focus is on technical, political, and legal aspects.

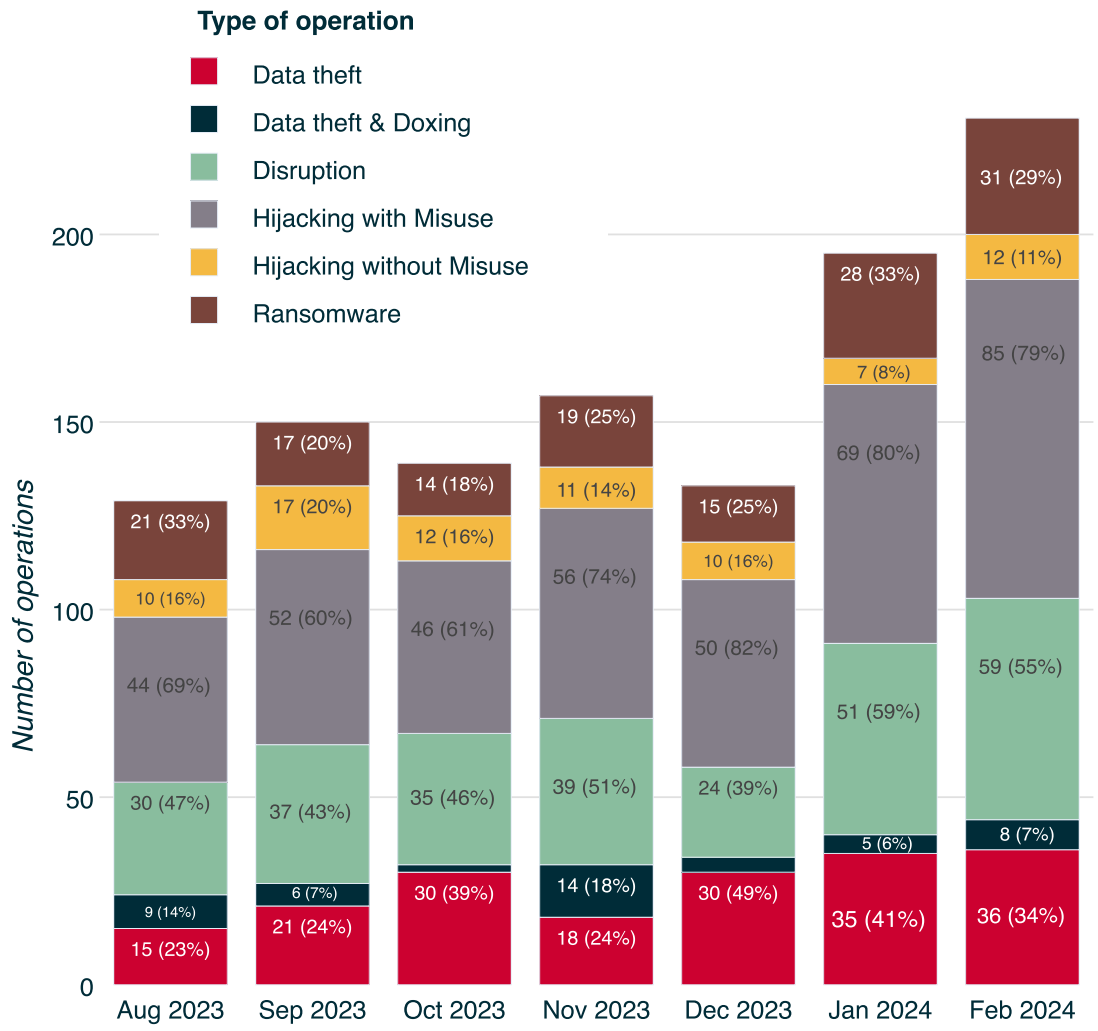
About EuRepoC

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

The incidents recorded in February 2024 are distributed across the following **operation types**:

Monthly distribution of operations



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

In February, the predominant activity observed consisted of **"hijacking with misuse"** operations, comprising 85 cases, which accounted for 79% of the total. As an umbrella term, this describes operations in which threat actors have succeeded in infiltratinh systems and networks to carry out unauthorised, harmful actions. Where feasible, EuRepoC distinguishes these activities based on threat actor intent and, when applicable, identifies data breaches or operational disruptions.

Amidst elections scheduled in over 60 countries this year, election-related entities have emerged as focal points not only for potential state-sponsored influence campaigns and espionage but also for financially-motivated cybercriminal activities. Disruptions in electoral processes and consequent delays in vote tabulation could affect the perceived legitimacy of results, presenting ransomware groups with opportunities for leverage. Extortion attempts may aim to paralyse systems or encrypt databases crucial for unimpeded voting.

In additional, confidential information of candidates represents a high-value target. During election campaigns, the release or mere threat of disclosing internal documents can exert considerable pressure, providing criminal groups with opportunities for profit. In this dynamic environment, state actors may seek to obscure actions intended to obtain and circulate compromising information by masquerading as ransomware operators.

In late January, the ransomware group Knight claimed to have obtained data from the networks of the Romanian Chamber of Deputies, the lower house of parliament. Albeit of relatively small size, the data set of 300MB contained copies of the identity cards of the Prime Minister and at least one other high-ranking politician.

Among the 316 total files were both publicly available information and internal documents from other parliament members. Initial reports suggested the stolen cache included bank information and patient data. Knight demanded the equivalent of 30,000 euros for the deletion of the data. Notably, Romania is scheduled to hold four rounds of elections in 2024, including for the presidency, parliament, European Parliament, and local offices.

To mitigate the threat of ransomware targeting critical election-related entities, the US Cyber Command initiated action as early as 2020 against the Trickbot botnet, a vehicle for malware distribution. This intervention, conducted ahead of the US presidential election, marked the first publicly disclosed instance of a "defend-forward" operation.

The second most common type of operation identified in February was **"disruption"** operations (55%). These operations aim to disable information technology services, thereby interfering with their availability. Typically, disruption operations are of a temporary nature. In the case of ransomware, however, blocked access to critical data can also cause downtime over a longer period of time. EuRepoC recorded 59 of these operations in February.

In mid-February, for instance, Izumi Co., Ltd., a company which operates supermarkets and shopping centres throughout Japan, was the target of a ransomware attack, prompting the closure of its shops for at least four days. Furthermore, the planned opening of a new branch scheduled for the beginning of March had to be deferred until the end of April due to the attack. Severely restricted access to accounting data and ordering systems caused prolonged delivery problems. The IT integration as part of a business merger with another food retailer, which was also planned for March, is expected to be delayed by three months due to recovery efforts.

While the management assesses the financial impact of the ransomware incident as low, the encryption of operationally important data is hindering the completion of the annual report for the 2023 financial year, due in April. The publication of the report had to be postponed indefinitely.

Similar constraints earlier affected the operations of at least two companies in Germany. Following a change in requirements of the German Stock Exchange, companies listed in the major German stock indices are obligated to submit audited annual reports by April of each year. Hurdles to meeting this reporting

obligation have the potential to cause distortions on financial markets. Last year, the biotechnology company Evotec faced temporary exclusion from the mid-cap index MDax after it was unable to submit its financial figures on time as a result of a ransomware attack. Battery manufacturer Varta missed the deadline this year due to an unspecified cyberattack and will likely lose its position in the SDax.

These instances underscore the broader financial ramifications of disruptive cyber operations, extending beyond immediate delivery disruptions for affected companies. The costs of such a forced exit from a prominent index may add to the damage caused by operational losses. Investment funds that mirror indices adjust their portfolios in response to changes in their composition, selling shares when companies depart from a benchmark. As triggers for wider divestment, index departures can have a longer-term influence on the share value, especially if affected companies no longer meet the criteria to return to the index after completing their financial reporting.

Focal points and targeting patterns

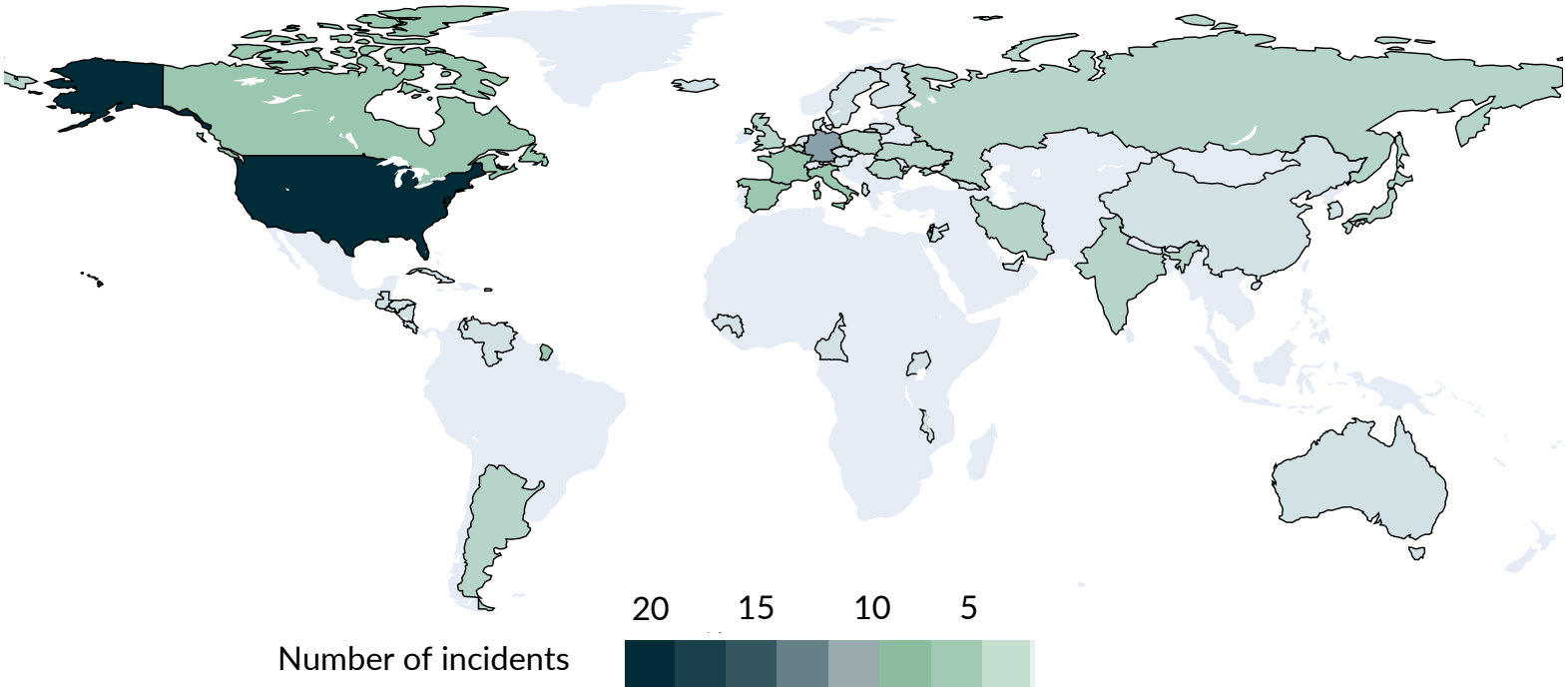
As observed in previous months, critical infrastructure companies registered again as the most affected sector in February 2024. With 56 cases, constituting 52% of newly recorded cases, this represents a slight increase in absolute terms, but a relative decrease of 10% compared to the overall rise in case number. State institutions were the next most frequent targets, with 47 cases (44%). This marks a minimal increase of two cases compared to the previous month but represents a relative decrease of 5%.

Although of lower intensity than the cases targeting critical infrastructure and state institutions, nine cases were recorded against end users and non-state targets, as well as the education sector in February, which represents a notable increase compared to previous months. Among cases against end users/non-state targets, operations by the US authorities against criminal actors stand out, which are described in more detail below, along with actions against Israeli targets attributed to Iran and Hamas, as documented in a report by Google's Threat Analysis Group and Mandiant. European universities and North American schools were particularly affected within the education sector (additional operations against public schools are tracked by EuRePoC as activities against the civil administration; research-intensive universities are covered as research institutions).

The United States continues to lead the list of most frequently affected countries. The 24 new cases recorded in February against the US account for around 22% of the total, representing a decrease compared to previous months. Germany follows the US with twelve recorded incidents. Two other member states of the European Union, France and Spain, as well as Israel, are the third most frequent target, with six incidents each. In contrast to previous months, the number of incidents affecting EU member states in February (39 cases in total) noticeable exceeds the figures for the United States.

For critical infrastructure targets, the healthcare sector was the most affected, experiencing 16 incidents. The distribution of these incidents is roughly evenly split between North America and Europe. Noteworthy attacks in February targeted service providers in the sector, some with

Geographic distribution of operations



far-reaching consequences. For example, a cyber incident at Change Healthcare, a subsidiary of the US insurance company UnitedHealth, caused far-reaching problems for pharmacies in prescribing medication. In France, the payment service providers Viamedis and Almerys were affected by the theft of the data of around 33 million individuals, roughly half of France's population. A ransomware incident at a Romanian IT service provider serving medical institutions also caused widespread outages in 25 hospitals, while the systems of a further 75 were shut down as a precautionary measure. The incidents underscore the intricate dependencies in the medical sector. Sector-wide reliance of health insurance companies, hospitals, doctors' offices on a few technical service providers can be the source of cascading consequences. Moreover, healthcare data's inherent sensitivity makes the sector especially attractive to criminal actors, as evidenced by sustained high rates of ransomware incidents against individual organisations.

The financial sector experienced twelve incidents, while the telecommunications sector was affected in ten cases. Notably, traditional financial institutions were increasingly targeted in February. Mirroring the trend observed for critical infrastructure entities, these institutions are increasingly impacted by ransomware incidents and/or data theft. In contrast, activities against the cryptocurrency sector revolved around financially-motivated "crypto heists."

Among state institutions, administrative authorities were the most affected, with 31 incidents. Additionally, apart from educational institutions, administrative bodies at local and regional levels were similarly affected. From a technical perspective, slightly over half of the incidents manifested as disruptions, with ransomware being reported in eight instances.

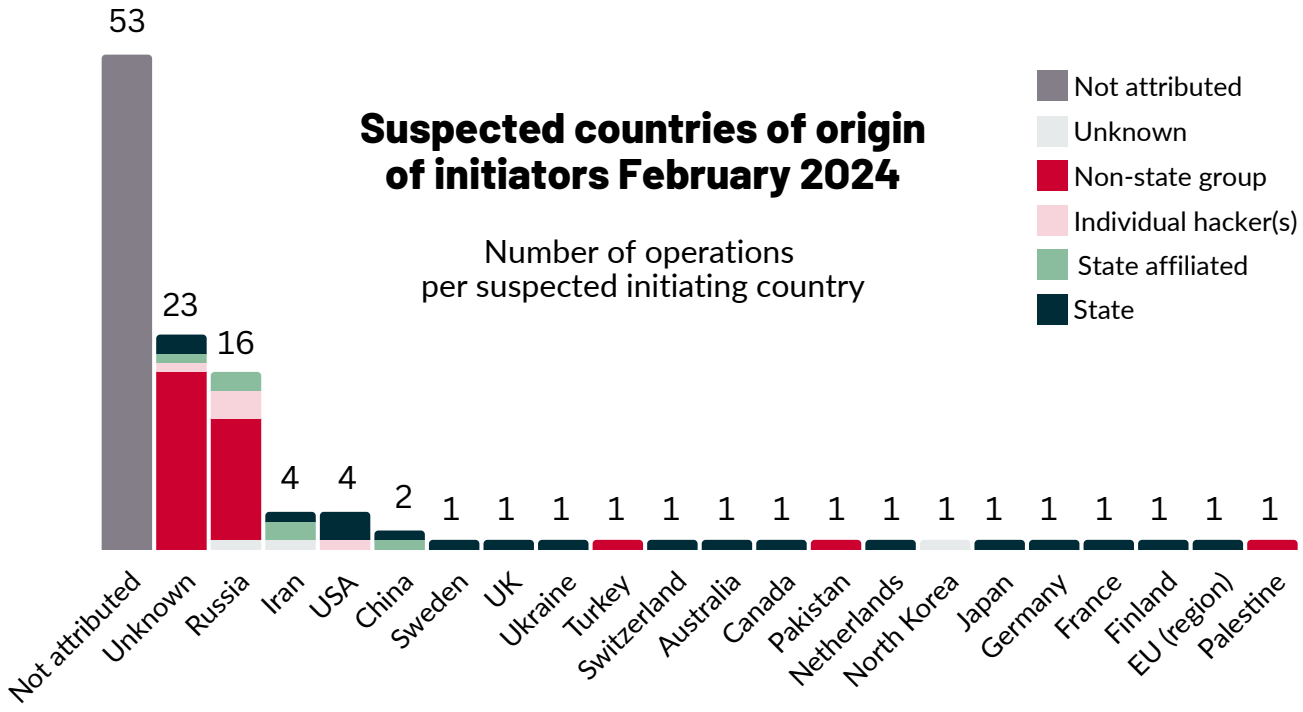
Threat actor profiles and attributions

In February, half of the total recorded cyber incidents remained unattributed to a specific country or type of attacker, amounting to 53 cases. However, incidents attributed to a specific type of attacker, albeit not to a country of origin, comprised 19% of cases (21 incidents), representing only a 4% decrease from the previous month. Notably, upon examining the list of attributed countries of origin, further differentiated according to the attributed actor types, a diverse array of countries emerged, with many countries being attributed in just one case each in February. However, a closer examination of the data reveals that a particular cyber operation, emphasizing defensive rather than offensive intentions, largely accounts for this: the takedown of the Lockbit ransomware group's infrastructure under "Operation Cronos." This operation entailed the dismantling of the group's leak site, the confiscation of its servers, and the arrest of two individuals. Apart from the US, law enforcement authorities from ten other primarily European countries participated, with Europol assuming a primarily coordinating role—a critical task given the involvement of over 20 authorities and the measures implemented by them.

Incidents attributed to non-state actors (e.g., hacktivists, cybercriminals, or individual hackers) increased by 10% compared to the previous month, accounting for 37% of cases. Among these, 18 were deemed criminally motivated. Relative to the overall cases, the proportion of cybercrime incidents remained nearly constant at around 18%. This also holds true for the 13% of incidents in February attributed to ideologically or politically motivated actors (hacktivists or patriotic hackers).

Conversely, the proportion of proxy operations, carried out by state-affiliated actors, decreased slightly from 7% in January to 6% in February.

Excluding the countries listed for their participation in Operation Cronos, the US remains salient, with four operations attributed to it. Three of these are linked to state actors. While these incidents meet EuRepoC's technical inclusion criteria, meaning a documented violation of the "CIA Triad of Information Security" (Confidentiality; Integrity; Availability), all were defensive in nature in terms of their functional orientation. Apart from the high-profile campaign against Lockbit, two other recent US actions against threat actors have garnered attention, particularly domestically. In one instance, the US Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) gained access to the Moobot botnet. The authorities then copied and deleted data from the infected routers and blocked the botnet's remote access to said routers under "Operation Dying Ember". The second case also involved an operation against a botnet consisting of infected small-office/home-office (SOHO) routers. This botnet was controlled by the Chinese group Volt Typhoon. FBI Director Christopher Wray described the infiltrations of US critical infrastructure targets as "prepositioning" operations at a hearing of the House of Representatives' Select Committee on the Chinese Communist Party. This hearing coincided with the announcement of the operation. Botnets can be misused not only for espionage, but also to cover up the compromise of critical networks and preserve access for possible disruptive operations in the future. The US administration identified Volt Typhoon's activities as such a preparatory measure and source of concern, particularly in view of a possible rise in tensions in China's relations with Taiwan.



The trend of states disclosing their "cyber countermeasures," underscores the self-image of democratic states, such as the US. States have a dual incentive to publicize their defence-oriented operations, to demonstrate their (presumed) successes to a domestic audience, and to present their own actions stopping malicious activity as supporting norms of responsible behaviour. Transparency about these operations is further supported by the court rulings that provide their legal basis. For instance, US Deputy Attorney General Lisa O. Monaco described the Volt-Typhoon operation as a threat to national security that was addressed "in real time." Similarly, the action against the APT28-hijacked Moobot botnet was depicted as a threat to US national security, situated in the context of Russia's actions against Ukraine. DOJ press releases for both operations described the respective actions of China- and Russia-nexus actors as destabilising and a threat to national security. However, the statements did not make any direct reference to the (voluntary) norms of responsible state behaviour in cyberspace recognised by UN member states. The official communications also did not include a direct reference to potential legal violations.

This strategic ambivalence between the general recognition of norms and the applicability of international law in cyberspace on the one hand, and the lack of public and concrete identification of breaches of norms/legal violations on the other, reflects a continued reluctance of states with highly developed cyber capabilities, such as the USA, to limit own actions in the long term. In this respect, democracies may refrain from linking autocratic actors' activities to a legal/norm violation to avoid constraining their own future actions. The seventh session of the UN Open-Ended Working Group (OEWG), which regularly allocates a separate session block to this topic, made it clear that the question of how exactly international law should be applied in the event of cyber conflicts remains one of the most pressing at international level, albeit with only moderate progress to date.

Conversely, autocratic states have so far not disclosed defensive cyber operations. This contrasts with the use of tools designed for digital repression, deployed against dissidents or political opponents. If at all, these measures are only procedurally based on national laws or court rulings and

typically frame the actions as fighting counter-terrorism, child pornography, or addressing drug-related crimes.

In February, a total of eleven cyber incidents were linked to conventional conflicts as tracked by the HIIK Conflict Barometer. The Russian war against Ukraine retains the highest profile, with five cases, followed by two operations related to the conflict between Israel and Hamas. The remaining four cases are divided among other longstanding dyads, albeit with significantly lower conflict intensity than the first two (China-Japan; China-USA; India-Pakistan). Additionally, one cyber operation was linked to internal tensions in Iran.

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

Jakob Bund is an Associate at the German Institute for International and Security Affairs (SWP).

Kerstin Zettl-Schabath is a Researcher at the Institute of Political Science (IPW) at Heidelberg University.

Martin Müller is a University Assistant and a doctoral candidate at the Institute for Theory and Future of Law at the University of Innsbruck.

Camille Borrett is a Data Analyst at the German Institute for International and Security Affairs (SWP).

Follow us on social media

@EuRepoC

linkedin/EuRepoC

contact@eurepoc.eu

https://eurepoc.eu