European
Repository of
Cyber Incidents

EuRepoC Cyber Conflict Briefing

May 2024

Jakob Bund
Kerstin Zettl-Schabath
Martin Müller

Overall observations

In **May 2024**, EuRepoC documented 73 cyber operations, representing a 21.5% decrease compared to the previous month. This figure is four incidents higher than the overall average in recorded activity of 69 operations per month.

The **average intensity** of operations in May 2024 registered at 2.92, surpassing the historical average of 2.83. The elevated level of operations documented by the Repository since February 2023 is partly attributed to expanded inclusion criteria. As of March 2023, EuRepoC has systematically recorded 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

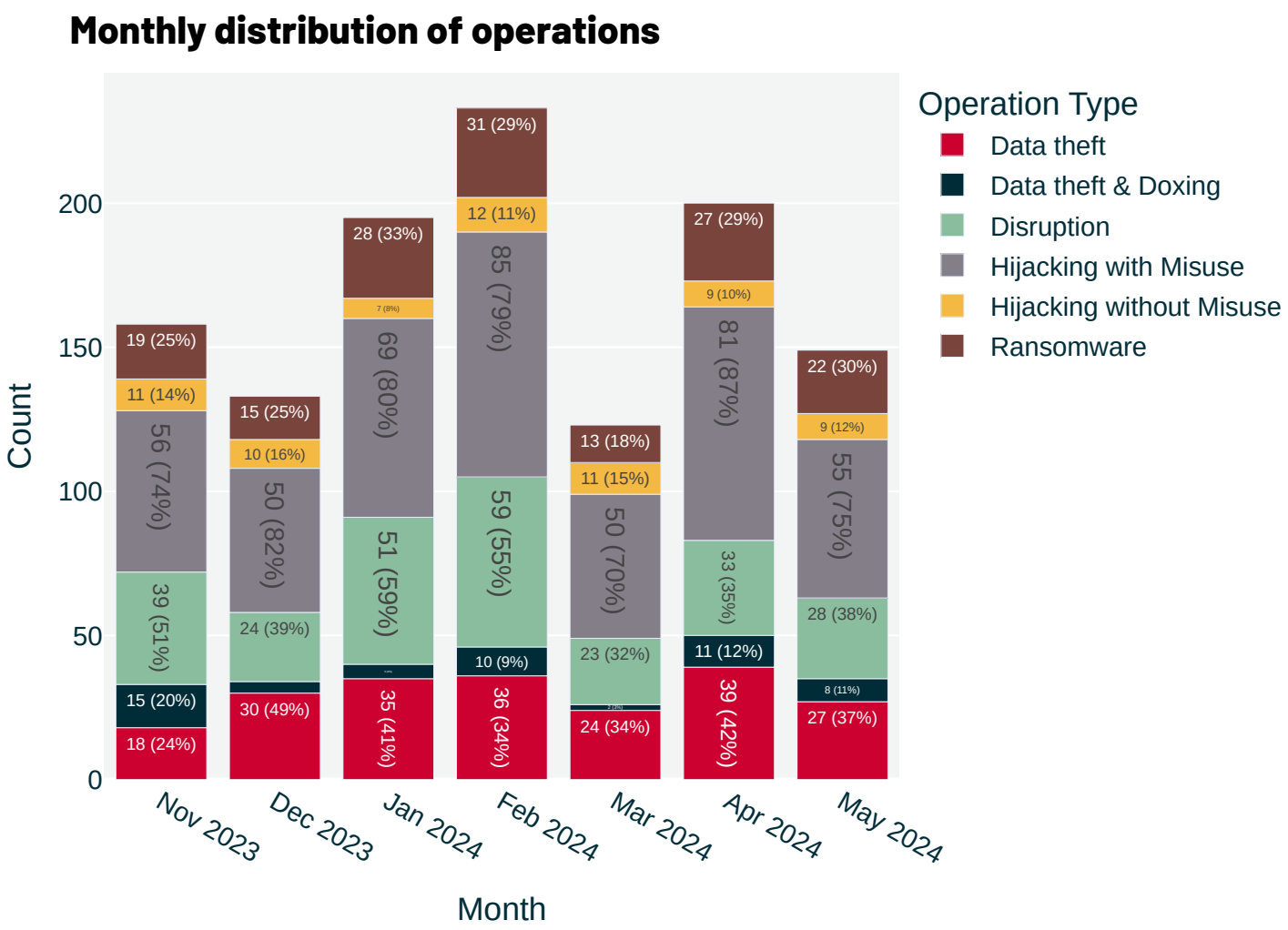
The Cyber Conflict Briefing is an analytic product prepared by EuRepoC. The German edition is published in collaboration with the **Tagesspiegel Cybersecurity Background,** accessible here.
It summarises the key trends, dynamics, and findings on cyber incidents as recorded by EuRepoC in a given month. These do not necessarily have to have taken place in May, 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 May 2024 are distributed across the following **operation types**:



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

In April, the predominant activity observed consisted of **"hijacking with misuse"** operations, comprising 56 cases and accounting for 77% of the total. This category encompasses operations wherein threat actors successfully infiltrate systems and networks to execute unauthorized and harmful actions. EuRepoC differentiates these activities based on the intent of the threat actors and, when applicable, identifies instances of data breaches or operational disruptions.

At a low-threshold level, such operations can target individual user accounts. For instance, on 10 May, unknown actors gained access to the X account of French Sports Minister Amélie Oudéa-Castéra, whose department is responsible for organising the Summer Olympics, set to open in Paris on 26 July.

In this instance, the intruders used the compromised account to send phishing messages to other users on the platform. Social media accounts with significant reach or official authority, such as those of politicians, also represent attractive targets for manipulation attempts, especially by groups aiming to instil a sense of uncertainty and vulnerability in the public. Major events like the Olympic Games that focus public attention provide an opportunity to scale up such attempts.

Similarly, news about a fictitious emergency situation can be disseminated quickly, at least initially, with minimal effort using hijacked accounts, particularly when messages are distributed via channels chosen for their broad broadcasting capabilities. Such attempts to spread misinformation can be swiftly identified. Their immediate impact, however, is often challenging to manage in real time, where threat actors aim to cause short-lived panic, embarrass security authorities and the host government, or to amplify public anxiety against a backdrop of serious threats of sabotage.

Russia, for example, has repeatedly attempted to stage terrorist threats under false flags in the past. In 2015, APT28 disrupted the broadcast of the French television station TV5Monde and published Islamist propaganda on its social media channels. The threat actor, attributed to the Russian military intelligence service GRU, posed as an affiliate of the Islamic State under the alias "Cyber Caliphate." In 2018, the Sandworm group, also presumably controlled by a GRU unit, targeted the Winter Olympics in South Korea with the intention of disrupting the opening ceremony with a wiper attack.

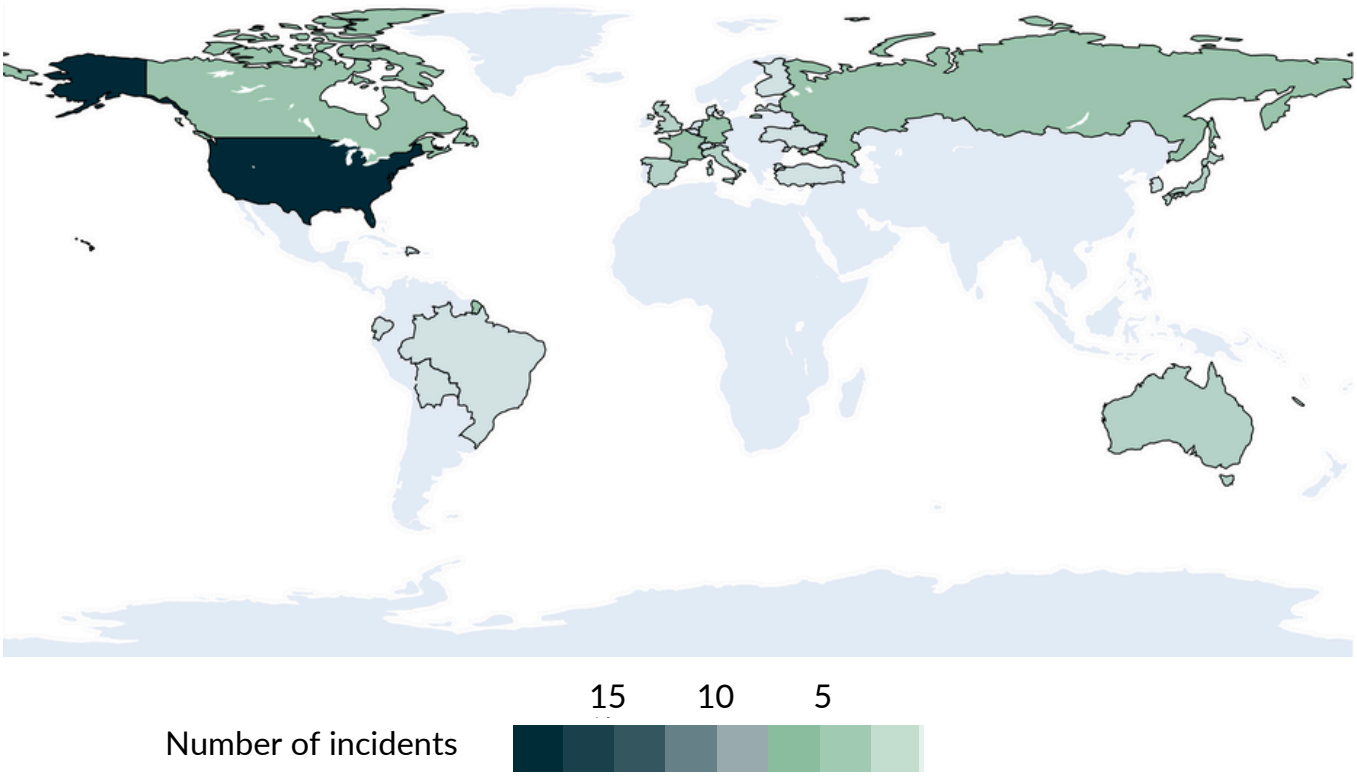
The second most common type of operation identified in May 2024 was "disruption" operations (38%). These are operations aim to put a service out of operation, impairing the availability of a service or product. Disruption operations are generally temporary in nature. However, in the case of ransomware, blocking access to critical data can also cause prolonged outages. The Repository recorded 28 such disruption operations in May.

Using relatively unsophisticated distributed denial of service (DDoS) tools, the Ukrainian military intelligence service HUR managed to suspend the transmissions of telecommunications providers in Tatarstan, one of the most populous autonomous republics in eastern Russia, on 3 May. The intermittent network outages affected providers MTS, TATTelecom, and regional operator Ufanet. These disruptions were concentrated in the Alabuga economic zone, which houses over 30 facilities, including several critical defence industry companies.

Even primitive actions such as DDoS attacks can restrict the flow of information or obstruct communication in the short term, despite the general ease with which such attacks can be mitigated. In the context of a major event, timed attempts to deliberately circulate false reports about an emergency, coupled with DDoS attacks against central news portals or government communication channels could contribute to a public sentiment of insecurity. In a similar scenario in March, the websites of authorities and ministries were inaccessible for several hours following a DDoS attack by the self-proclaimed hacktivist group Anonymous Sudan on the French interministerial digital agency (DINUM), which is responsible for managing more than 300 government domains.

The combination of DDoS attacks alongside social media account takeovers can form part of a deliberately simple toolkit that is generally plausible for hacktivists to use. State actors may seek to leverage these tools and tactics through hacktivist cutouts to obscure their responsibility, or at least deny accountability to selected audiences. DDoS campaigns by hacktivist organisations with suspected links to Russia, such as Anonymous Sudan, NoName057(16), or KillNet, demonstrate ongoing efforts to play up the minor impact of these actions. By inflating the significance of these minor disturbances, these groups seek to foster ear, uncertainty, and doubt among their

Geographic distribution of operations



targets, thereby looking to achieve a psychological advantage. This approach leverages the relatively low-cost nature of the attacks to generate disproportionate media coverage and public concern, amplifying their influence beyond the actual technical damage inflicted.

Focal points and targeting patterns

The most frequently affected target sector in May 2024 was critical infrastructure, which was targeted in 44 new cases (60%). Government institutions were the second most affected, with 26% and 36% of cases. This represents a decrease of 17% for critical infrastructure and 38% for state institutions compared to April.

The number of recorded incidents for businesses not considered critical infrastructure also remained high: While EuRepoC does not systematically account for incidents against such corporate targets beyond critical infrastructure, the Repository tracks cases where these incidents fulfil other inclusion criteria. Such cases may for example be included in the database because of a "politicisation" of the event, when an incident can be attributed to a political actor or has become part of the public debate. A case may also be included if a company was targeted as part of a wider operation against entities that directly meet EuRepoC inclusion criteria, such as incidents involving critical infrastructure operators. This was the case for six incidents in May.

The United States, as in previous months, was the most frequently targeted country, this time in 20 cases. With 19 incidents, EU member states were affected almost as often. France was targeted in five incidents, followed by Germany with four and Italy with three.

Looking at affected critical infrastructure sectors, the healthcare sector continued to be targeted the most, in overall nine incidents. Although ransomware groups were only identified as the suspected perpetrators in two of these cases, several

factors suggest that criminal groups are behind the remaining incidents. Geographically, these operations show a notable focus on North America, consistent with previous observations. For almost all incidents, affected organisations and subsequent media coverage reported data theft.

One exception is the incident at prescription service provider MediSecure in Australia, which was first publicly disclosed by National Cyber Security Coordinator. Given the considerable volume of data affected, with estimated ranging around 6 terabytes, the incident resembles the data breach at health insurer Medibank in October 2022. Earlier this year, Australia, the UK, and the United States responded to the Medibank incident with joint sanctions against one of the suspected perpetrators.

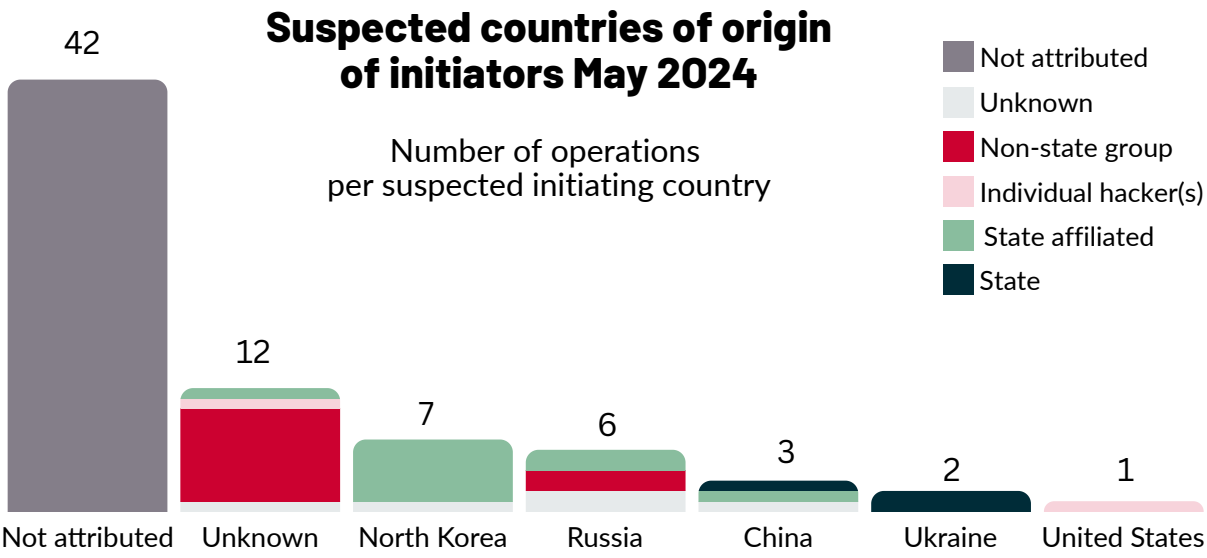
The energy sector and critical manufacturing were the second most affected critical infrastructure sectors, counting seven incidents each. As in other industry verticals, ransomware manifests as a persistent threat to the energy sector. In May, the Repository also recorded an increasing threat from self-proclaimed Russian hacktivists, potentially operating as cover for Russian intelligence services. Several US authorities reported attempts by these actors to compromise local operators of water and waster water systems, as well as other critical infrastructure targets, for disruptive purposes via control systems that can be accessed online.

Ransomware also remained a threat to the critical manufacturing sector, as demonstrated by cases targeting US optics manufacturer Omnivision and Nissan North America. As reported for Volkswagen in last month's briefing, cases of industrial espionage pose a serious risk in this sector. The Moonstone Sleet group highlights these risks. Attributed to North Korea, this group has targeted several companies in the aviation sector since December 2023, aiming to acquire technological know-how.

In the case of state institutions, 16 incidents indicate that lower-ranking administrative units continue to be more frequently targeted than national institutions. In one such case against a sub-national institution, the Hessian University for Public Management and Security in Germany was targeted in a ransomware attack. Conversely, nine incidents were recorded at higher administrative levels in May. Notably, a compromise of Shared Services Connected, a service provider for the British security and defence authorities, resulted in leaked payroll data for the British armed forces. Additionally, the FSB-associated Russian APT group Turla is suspected to have stolen data from an unnamed European foreign ministry. Only recently disclosed, the intrusion potentially traces back to 2020.

Threat actor profiles and attributions

At 58%, the proportion of completely unattributed incidents increased by 9% in May compared to the previous month (49% of cases). The proportion of operations that were specified in terms of attacker type but not by country of origin fell from 24% in April to 15% in May. The list of recorded countries of origin of incidents added to the database in May, on the other hand, has dropped sharply compared to April. Besides Iran, it primarily includes the most frequently attributed autocracies, as well as Ukraine and the USA. For the case originating in the US, distinct personal motivations appear responsible.



A student from Texas allegedly used his school laptop to initiate DDoS attacks, disrupting Internet services during the district's state mandated testing (STAAR). This affected all schools within the district and impacted approximately 3,000 students who had to pause and restart their tests. The next day, 700 students had to be excluded from the tests and needed to retake the exam due to continued disruptions. The case illustrates two key points: firstly, it demonstrates how easy it has become even for individuals with limited technical skills to carry out DDoS attacks. This trend is likely to intensify as AI-supported applications make more advanced tools and techniques accessible, enabling individuals with limited training to conduct more complex operations. Secondly, cyber operations are carried out by a variety of perpetrators, including insiders who may disrupt systems and cause damage. A recent example of such a case involved a disgruntled ex-employee who accessed his former company's computer systems and deleted 180 virtual servers, causing 918,000 Singaporean dollar ($678,000) worth of damage. On 10 June, the man was sentenced to two years and eight months' imprisonment for unauthorised access to computer material. The case points to the contributions to corporate cyber hygiene of HR-related measures, such as account management, that may originally not have been designed for security.

With respect to attributed state operations, Ukraine continued its strategy of disclosing its own offensive operations against Russian targets. On 7 May 2024, Ukrainian military intelligence disrupted the Russian software developer 1C and the cloud provider Cloud4y. Previously, HUR had also claimed responsibility for an Internet outage in Tatarstan on 3 May, as detailed above. In both cases, the operations were self-attributed through anonymous intelligence sources. One reason for disclosing these activities through leaks to the media rather than official statements may be that both targets - the software company and the telecommunications providers - were civilian entities and therefore not legitimate targets of malicious operations in the context of military conflicts from the perspective of international law. In past instances involving activities against Russian government entities, HUR had released press statements.

Ukrainian allies, including Germany, and international organisations such as the International Committee of the Red Cross, view military operations against civilian targets as justifiable under international law only if it could be proven that the systems attacked had been used directly for military purposes. Critical infrastructure entities, including telecommunication providers, are further subject to special protection, as endorsed by all UN member states through norms for responsible state behaviour in cyberspace during peacetime. Notably, Russian actors have launched devastating physical attacks against critical infrastructure and civilian targets, in addition to cyber operations. Against this backdrop, Ukraine's actions show that democratic states face complex cost-benefit considerations when using cyber operations in a military context, including with regard to the communication of their own operations.

Russia's war against Ukraine continued to dominate for cyber operations in the context of conventional conflicts. In May, these activities accounted for seven incidents. In addition, two other conflict dyads were recorded, each with one associated cyber operation. This included North Korea-South Korea and Vietnam/et al.-China in the context of the South China Sea disputes. The latter case appears noteworthy for several reasons: First, Bitdefender blamed a previously-undocumented APT, which the company tracks as "Unfading Sea Haze," for a multi-year espionage operation against eight military and government targets in the South China Sea region. According to Bitdefender, the group's activities align with Chinese interests in the context of the territorial conflict, which, in addition to technical overlaps with Chinese APTs, provides for an initial attribution hypothesis.

Despite the recent revelation, Unfading Sea Haze is likely not a new formation but suspected to be a state-sponsored group that managed to evade detection for over five years. The group repeatedly compromised the same systems, highlighting the consequences of shortcomings in credential management and inadequate patching practices for public-facing devices or web services. Alleged Chinese cyber espionage in the context of this conflict follows a pattern of previously uncovered campaigns, not only against targets in Vietnam (the Repository currently includes 18 such cases against Vietnam for the period since 2005), but also against the Philippines (19 recorded operations, since 2005) or Malaysia (11 recorded operations, since 2011). By contrast, the far more frequent Chinese espionage operations against Taiwanese targets often cannot be clearly attributed to the bilateral conflict between China and Taiwan over the island's status on the one hand, or the regional conflict over the South China Sea on the other. The activities described demonstrate the strategic instrumentalisation of cyber operations by Chinese APTs in the context of numerous national and regional conflicts. However, the increasing integration of cyber capabilities into overarching military strategies under the direction of China's President Xi Jinping point to capability developments for what might be disruptive operations, including against military and critical infrastructure targets. The delineation of tasks within China's operational structure is again the focus of scrutiny following the dissolution of the PLA's Strategic Support Force (SSF). Established in 2015, the SSF consolidated the computer network exploitation and computer network attack mission sets previously housed in the third and fourth departments of the General Staff Department. In April, the PLA's Central

Military Commission announced the split of the SSF into three separate arms. While the Aerospace Force and Cyberspace Force oversee capabilities for their respective domain, the new Information Support Force is expected to serve information needs across the armed forces.

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.

Follow us on social media

@EuRepoC

linkedin/EuRepoC

contact@eurepoc.eu

https://eurepoc.eu