European
Repository of
Cyber Incidents

EuRepoC Cyber Conflict Briefing

November 2023

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

Overall observations

In **November 2023**, 76 cyber operations were recorded in the EuRepoC database. This is a 4% decrease from the previous month, yet 17 operations more than the overall average in recorded activity of 58 cyber operations per month.

The **average intensity** of operations recorded in November 2023 registered at 3.13, which is below the historical average (2.7). The striking increase in operations since February 2023 is partly explained by the fact that, since March 2023, EuRepoC has 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 October, but may have started earlier. The focus is on technical, political, and legal aspects.

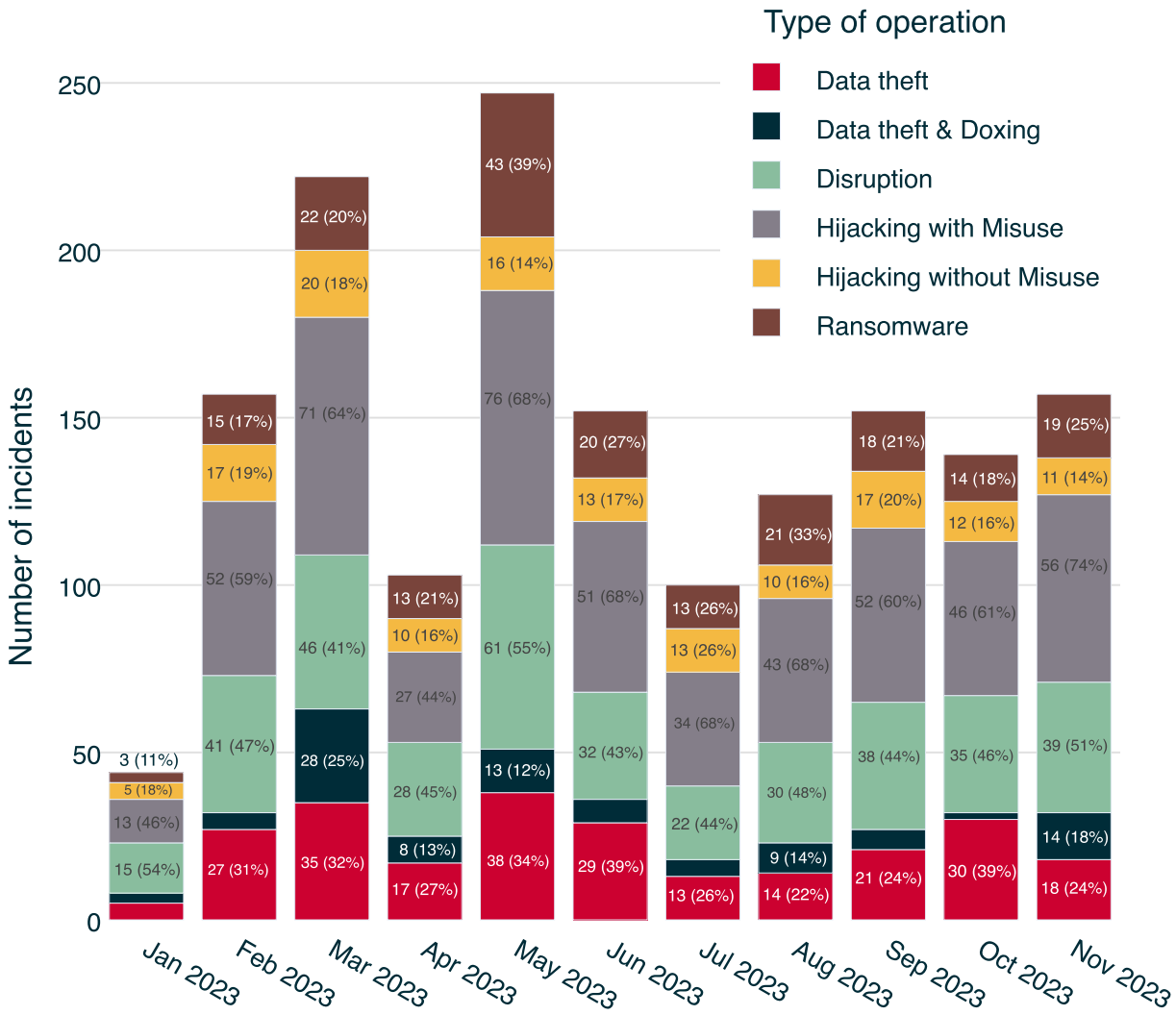
About EuRepoC

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 November 2023 are distributed across the following **operation types**:

Monthly distribution of operations



The largest share of activity tracked in November comprises **"hijacking with misuse"** operations, with 56 cases (74%). As an umbrella term, this describes operations in which threat actors have succeeded in penetrating systems and networks to carry out unauthorised, harmful actions. Where collection on these indicators is possible, EuRepoC differentiates these activities further by threat actor intent and, if applicable, identifies data theft or operational disruptions.

As discussed last month in connection with the case of StripedFly, an espionage operation disguised as a cryptominer, the assessment of motives, especially with regard to "hijacking with misuse operations," poses a continuous challenge even for activities that have been under observation for years. These difficulties may persist when an outflow of data can be detected for a certain operation, but the use of the stolen information is not immediately evident.

In a precedent-setting step at the end of November, the Ukrainian military intelligence service GUR not only disclosed an offensive cyber operation it had conducted and published data it had exfiltrated, but also used a press release describing the obtained material to emphasise the importance of international sanctions against Russia and to incorporate the operation's disclosures directly into its own strategic narratives.

Specifically, the GUR, according to these accounts, succeeded in penetrating networks through which it gained access to confidential reports from Russia's civil aviation authority, Rosaviatsia.

The reports, which cover a period of more than a year and a half and document safety-related incidents and malfunctions, indicate considerable difficulties in complying with maintenance requirements. According to these reports, almost 70% of the aircraft in Russian fleets can only be kept in working order through inspections in non-certified maintenance centres and through the use of non-original spare parts.

In the official communication on the operation, the GUR details findings that paint a devastating state of Russia's aviation safety and refers to the leaked data set. Against the background of this evaluation, the press release also asserted that international sanctions contributed significantly to this situation, highlighting bans on deliveries of aircraft and spare parts; the exclusion from software updates; the seizure of Russian aircraft abroad; and the restriction of access to meteorological information for air navigation.

According to the Ukrainian Ministry of Defence, the impact of sanctions was partly responsible for the September 2022 decision by the International Civil Aviation Organisation (ICAO) to add Russia to its "red flag" list, marking countries without sufficient safety oversight. Russia is just one among five countries with this status. In February 2022, the ICAO was also the first UN organisation to condemn Russia's renewed invasion of Ukraine.

The second most common type of operation identified in November was "disruption" operations (51%). This refers to operations with the aim of disabling an information technology service. In this regard, a disruption or interference impairs its availability. Disruption operations are usually temporary in nature. In the case of ransomware, however, blocked access to critical data can also cause downtime over a longer period of time. EuRepoC recorded 39 of these operations in November.

In the context of geopolitical tensions, sabotage attempts, in rare cases, have also been observed as part of disruption operations. The Russian threat actor Sandworm, for example, gained access to the operational control systems of a Ukrainian electricity organisation in June 2022 and destroyed data with a modified variant of CADDYWIPER the following October, as reported by the threat intelligence company Mandiant on 9 November 2023. CADDYWIPER was first observed by the cybersecurity company ESET in attacks against Ukrainian targets shortly after the Russian invasion in mid-March 2022.
Sandworm gained access to the target environment via a hypervisor, a software that simulates an independent computer environment.

Using this access, Sandworm was able to reach connected industrial control systems, known as SCADA systems, which the affected energy company was using to monitor substations. On 10 October 2022, the Russian group triggered the circuit breakers of a substation controlled via this system and caused a power outage.
In contrast to previous attempts to cut the Ukrainian power supply, Sandworm's most recently reported actions are characterised by efforts to achieve this goal using the target network's own tools wherever possible - a tactic commonly known as "living off the land."

These techniques aim at disguising malicious actions as supposedly normal operational behaviour. In addition to avoiding detection, protecting the group's own arsenal and preventing attribution of its own capabilities may have further motivated this approach - considerations that gain weight in view of developments in a war of attrition.

Two days after triggering the power outage, Sandworm caused another disruption by deploying CADDYWIPER in the electricity organisation's IT networks. As the wiper's scope was limited to the IT environment, this action had no direct impact on the systems responsible for maintaining the power supply. Although Sandworm had previously tried to cover up the traces of its own activities, the execution of the wiper drew attention, presumably unintentionally, to the causes of the already carried out cyber-enabled sabotage and may indicate a lack of coordination within the attack team.

Mandiant estimates that Sandworm was able to disrupt the OT systems critical to power delivery at least three weeks before the power outage was ultimately achieved.

The actual disruption to the power supply in October achieved through the interference with the substation's control systems overlapped with several days of rocket fire on critical infrastructure in Ukraine, including the city where the affected energy company is based.

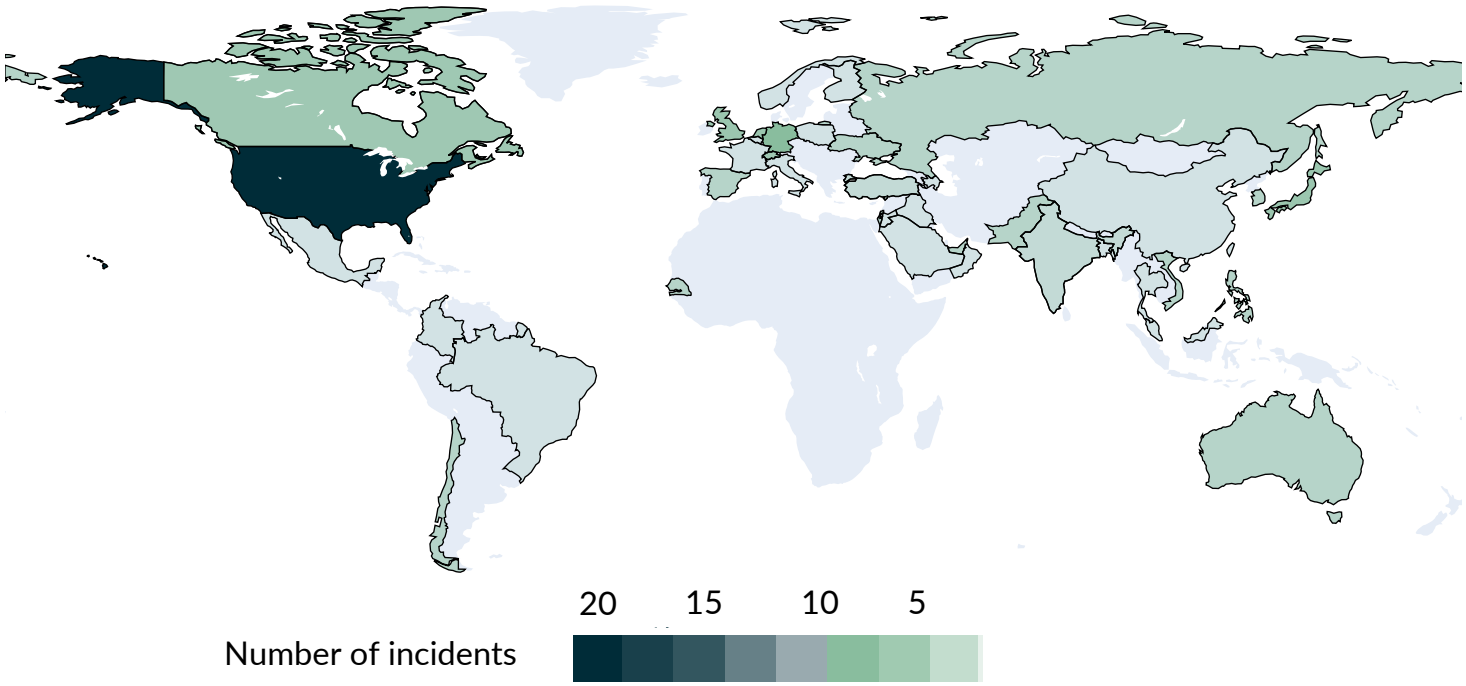
Considering the fact that Sandworm already had the opportunity to conduct the operation prior to this missile attack, the overlap in timing could indicate efforts to combine the use of conventional weapons with cyber capabilities. With regard to cyber operations, this combination may also offer the advantage of covering up the cyber-enabled cause, as in this example of the power outage, and preventing the premature discovery of the attack tools. Government agencies in the US, UK, and the EU have repeatedly drawn clear links between Sandworm and the Main Centre for Special Technologies (GTsST), also known as Unit 74455, which is part of the Russian military intelligence service GRU.

Focal points and targeting patterns

As in the previous month, the most frequently targeted sector in November 2023 was critical infrastructure companies, with 46 (60%) of the new cases. This is an increase compared to the 39 cases in October and is in line with previous months in relative terms, apart from the brief downward trend observed last month. The second most affected sector was state institutions, with 25 cases (33%), which represents a decrease of seven cases - or 10% - and thus also remains below the previous months in relative terms.

Among affected countries, the United States is again the most frequently targeted country, with 23 cases, accounting for 30% of all incidents recorded in November.

Geographic distribution of operations



This is followed by Germany, with seven incidents; almost a third of all cases recorded in November were cases in which EU member states were affected (18 in total). Japan was also frequently affected, with five incidents; the UK and the Netherlands were each targeted in four incidents; and Russia in three incidents relating to the war in Ukraine - discussed in more details below.

Within the critical infrastructure cluster, the healthcare sector was most frequently affected this month, with eleven incidents. Public reporting in most of these cases, however, did not identify the perpetrators behind the intrusions or whether the incidents involved the deployment of ransomware. Recorded incidents showed a prominent geographical concentration for US healthcare services. The persistence of malicious activity against the healthcare sector has prompted the responsible US authority to announce a sector-specific cybersecurity strategy in early December, which will take the increase in ransomware incidents into account. In Germany, a cyber incident at Esslingen Hospital was recorded for the healthcare sector, albeit without any report of ransomware use.

Among critical infrastructure targets, the telecommunications and critical manufacturing verticals remain frequently affected, with ten and nine incidents, respectively. Within the telecommunications sector, a spectrum of activity was observed, ranging from hacktivist actions - such as a DDoS attack on the website of the service provider Cloudflare or the disruption of Palestinian Internet servers - to data theft targeting Vodafone in Spain. Espionage operations by the Iranian threat actor Scarred Manticore, also directed against telecommunication companies, are analysed in more detail below.

In the area of critical manufacturing, the majority of cases can be attributed to ransomware groups, similar to the healthcare sector. While for data theft against organisations in the healthcare sector, the criminal actors' interest in particularly sensitive personal data appears to be the primary targeting motivation, in the area of critical manufacturing, this interest is linked to the intellectual property and knowhow held by individual companies. In November, such cases involved the aircraft manufacturer Boeing, the Japanese electronics manufacturer Sony and the Dutch chip manufacturer NXP, for example.

In the case of state institutions, both "Civil Service/Administration" and "Government/Ministries," with eleven and ten incidents, respectively, remain by far the most frequently affected. Within civil service targets, a familiar picture emerges, as evidenced by two incidents targeting educational institutions (including the British Library) and incidents targeting local institutions, such as several municipalities in the district of Neu-Ulm, the city of Neuss, or the Swiss municipality of Zollikofen.

For governments and ministries, a number of DDoS attacks can also be attributed to the conflicts in Ukraine and Israel, which affected the websites of Swiss, Belgian, and Bahraini government institutions, for example. Operations by several Chinese state-linked APTs against government authorities in Cambodia and the Philippines, which presumably pursued espionage objectives, also fit patterns of political motivation.

Threat actor profiles and attributions

In November, the majority of the cyber operations recorded had not yet been attributed to a country of origin, with the authorship still unclear in 70% of cases (53), which corresponds to the 70% average for this figure in previous months. In 25 of the 76 total cases, non-state actors were held responsible, which is 3% less than in the previous month of October. Of these 25 cases, criminal groups were identified as the perpetrators or claimed the operations in 14 cases, for example in the context of ransomware incidents. The remaining 11 cases involving non-state actors, on the other hand, tended to be politically- and ideologically-motivated. This relative distribution roughly corresponds to that of the previous month of October. As in previous months, both criminally- and politically-motivated operations were dominated by groups with Russian connections, for example with various hacktivist operations by the NoName057(16) group (3 DDoS attacks). The same applies to the criminal ransomware group Lockbit, also with three attributed incidents in November.

The list of attributed countries of origin of the attackers is characterised by a lower number/diversity in November compared to September, for example, when ten different countries of origin were identified. Regular listings are again observed in November: Russia, North Korea, Iran, and China - but also Ukraine, due to the involvement of non-state (as well as state) actors in cyber operations against Russian targets.

Six incidents were recorded in November for so-called "cyber proxies," i.e., hacker groups tolerated or tasked by states, but where the level of separation from state agencies can also become increasingly blurred. Three of such operations were attributed to Iranian groups and two to North Korean proxies. One case involved Chinese proxy activities. For Iran, the espionage case of the group documented by CheckPoint Security under the name Scarred Manticore stands out, as it has not previously been the subject of detailed threat intelligence reports. In the case in question, the group, which is believed to have links to the Iranian Ministry of Intelligence and Security (MOIS), gained access to the Windows servers of various state and private institutions in the Middle East using the LIONTAIL malware framework since at least 2022. Although Scarred Manticore is primarily described as an espionage actor, CheckPoint discovered connections to previous disruptive Iranian operations. Some of the tools used by Scarred Manticore are associated with the destructive attacks against the Albanian government infrastructure in mid-July 2023. As Microsoft has attributed responsibility for different phases of the operations against Albanian targets to different threat actors, whether this is merely a case of tool-sharing, which is becoming increasingly common among APTs of a shared state nexus, or whether Scarred Manticore was involved in the operations against Albania in a more active capacity warrants further analysis. The case illustrates the extent of geopolitically-motivated espionage that Iran has been conducting for many years now. State-controlled - or at the very least, state-directed groups - are accounting for this pattern, and according to threat intelligence reporting, these groups are competing for state contracts in an ever-growing ecosystem, as supported by the exposure of commercial and scientific institutions, such as the Mabna Institute, as Iranian cyber proxies. In most cases, the groups maintain links to either the Islamic Revolutionary Guard Corps or the MOIS.

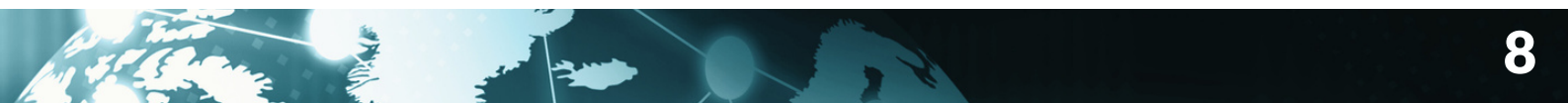
Government agencies in one country officially admitting to having compromised targets in another is a notable exception. In the past, the US has made statements about its own cyber operations in select cases, including an operation against the Internet

Research Agency in St. Petersburg as a preventive measure before the 2018 midterm elections, or statements leaked via media reports about cyber operations against Iranian targets in the context of tensions in the Strait of Hormuz in 2019. The fact that a military intelligence service, as described above for the case of the Ukrainian operation against Rosaviatsia, has itself publicised a hack-and-leak operation on its own website and also disclosed comprehensive information obtained through the operation in this form is unusual. Data points highlighted in official Ukrainian communications appear intended to show the impact of sanctions against Russia on the country's civilian aviation, which is likened to being on the verge of "collapse."

Official Ukrainian statements based on the obtained documents, which allege that the sanctions imposed on Russia are also affecting civil aviation, were confirmed by further media reports in the course of December. Hack-and-leak operations typically aim to influence internal decision-making processes of a foreign country from behind a veil of "plausible deniability," for example in the run-up to national elections. To this effect, perpetrators strive to hid their identity, as this has the advantage that the public focus remains on the content of the leaks. On the other hand, state actors are likely well aware where operations under their remit cross norms and legal thresholds, including violations of another country's sovereignty or the of principle of non-intervention in peace times. In the context of an international armed conflict, as in Ukraine, international humanitarian law supersedes these considerations, which, among other things, requires special protection of civilian infrastructure. At least three reasons may help explain why the Ukrainian government decided to make details of the operation public: first, it may not see its actions as illegitimate in the face of Russia's initial aggression, which precipitated the armed conflict in the first place, but rather as a necessary and justified measure under its right to self-defence. Second, the public component of the hack-and-leak operation may be part of an effort to address the Russian population to illustrate the negative consequences of the Kremlin's war of aggression for the Russian population, in this case travel safety. Third, the action could also be interpreted as a signal to Ukraine's allies regarding the benefits of the sanctions imposed to ensure their continued support.

The attribution that received the most attention in November, also against the background of the aforementioned limits of international humanitarian law, was the above-mentioned Mandiant report about Sandworm's sabotage operation against Ukrainian energy infrastructure in October 2022.

As in October, the conflicts between Ukraine and Russia (10 incidents) and Hamas and Israel (3 incidents) dominated the cyber operations landscape in November for incidents which the repository was able to assign to existing conventional conflicts as recorded in the Conflict Barometer of the Heidelberg Institute for International Conflict Research (15 out of 76 in total). An additional case relates to the Iran-Israel conflict dyad. A suspected August 2023 cyber espionage incident by the Chinese APT Mustang Panda against government targets in the Philippines is attributed to the overarching conflict between numerous littoral states in the South China Sea region. The incident was immediately preceded by a clash between the Chinese coast guard and a Philippine ship.



In line with the advantage afforded by cyber operations that they usually do not require developing a physical presence in target countries through human operators, the three conflict dyads mentioned above show that different forms of cyber operations are used, particularly in the context of regional conflicts with varying objectives, depending on the respective escalation status of the conflict.

More from EuRepoC

In addition to the daily Cyber Incident Tracker and the EU Media Reporting Tracker, EuRepoC as of December also offers an Attribution Tracker on the project website. This resource provides quantitative and qualitative figures and categorisations of the attributions recorded over the last six months. The data is updated on a monthly basis in order to identify short and long-term attribution trends on both a European and international level.

EuRepoC provides information about new cyber incidents added to the database with a daily curated Cyber Incident Tracker - open to free subscription 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