European
Repository of
Cyber Incidents

EuRepoC
Cyber Conflict Briefing

September 2023

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

Overall observations

In **September 2023**, 86 cyber operations were recorded in the EuRepoC database. This is a 37% increase from the previous month, and 30 operations more than the overall average recorded activity of 56 cyber operations per month.

The **average intensity** of operations recorded in September 2023 is 2.5, 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 September, but may have started earlier. The focus is on technical, political, and legal aspects.

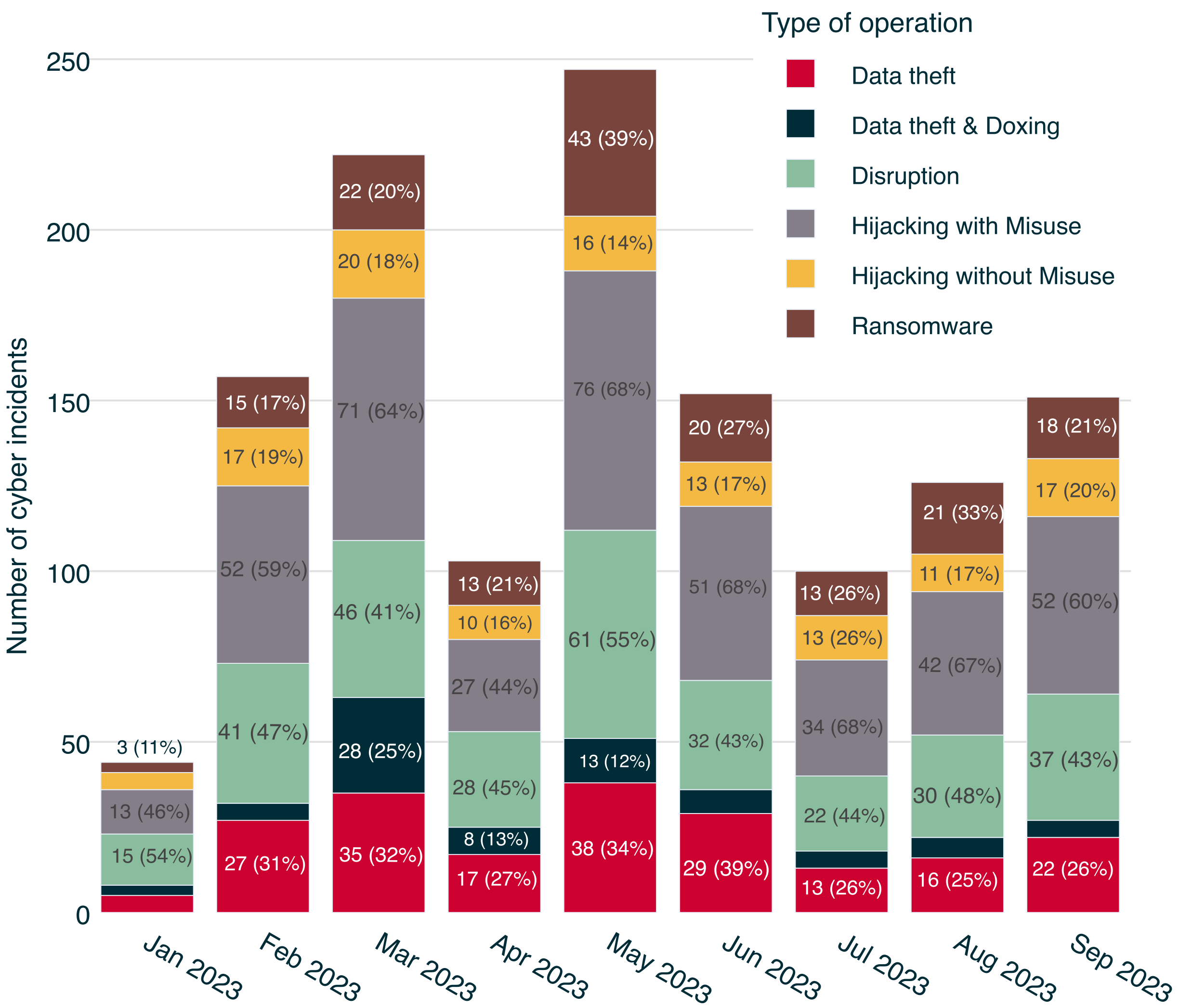
About EuRepoC

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

Monthly distribution of operations



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

The largest share of activity tracked in September comprises **"hijacking with misuse"** operations (60%). 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.

Cryptocurrency thefts have increased in prevalence among tracked hijacking operations. At the beginning of September, the FBI attributed the theft of the equivalent of $41 million USD from the online casino and betting platform Stakes.com to state actors from North Korea. The FBI specifically blamed the Lazarus Group for the theft, further referencing APT38. Past observations of the activities and tools attributed to the group suggest that Lazarus is a network of actors operating as part of the Reconnaissance General Bureau within the Korean People's Army - North Korea’s armed forces.

Lazarus-linked units operate particularly under the Third Bureau, which specialises in foreign intelligence gathering. One of these units is APT38, which operates with a focus on targets in the financial sector. In October 2023, the threat intelligence company Mandiant documented a prolonged operational pause for APT38. Subgroups such as CryptoCore (UNC1069) and TraderTraitor (UNC4899) continue to be active and focus on the theft of cryptocurrencies. Mandiant assumes the ranks of both groups have been bolstered by former members of APT38. Linking specific activities to individual subgroups and distinguishing between the operational profiles of subunits remains a challenge in part because North Korean operatives work from common physical locations due to their integration into military structures.

The FBI announcement from September uses the references to Lazarus and APT38 without further qualification. A previous FBI announcement in August identified TraderTraitor in connection with a series of thefts during the summer months, seemingly equating this subgroup with Lazarus and APT38 without providing more detail on a possible conceptual distinction.

To date, APT38 has been responsible for some of the biggest financial thefts in cyberspace, including the theft of almost one billion dollars from a Bangladeshi central bank account in 2016 through fraudulent instructions sent via SWIFT, a network that mediates financial transactions between banks. APT38 stands out in particular for its willingness to delete data from compromised networks in order to conceal any evidence of its own operations. As of mid-September 2023, North Korean groups are estimated to have stolen a total of $340.4 million USD in cryptocurrency, on track to surpass the financial losses caused in previous years.

The second most common type of operation recorded in September comprises "disruption" operations. This refers to operations aimed at disabling an information technology service. Accordingly, a disruption or disruptive operation affects the availability of data. Disruption operations are generally temporary in nature. EuRepoC recorded 37 such incidents in September.

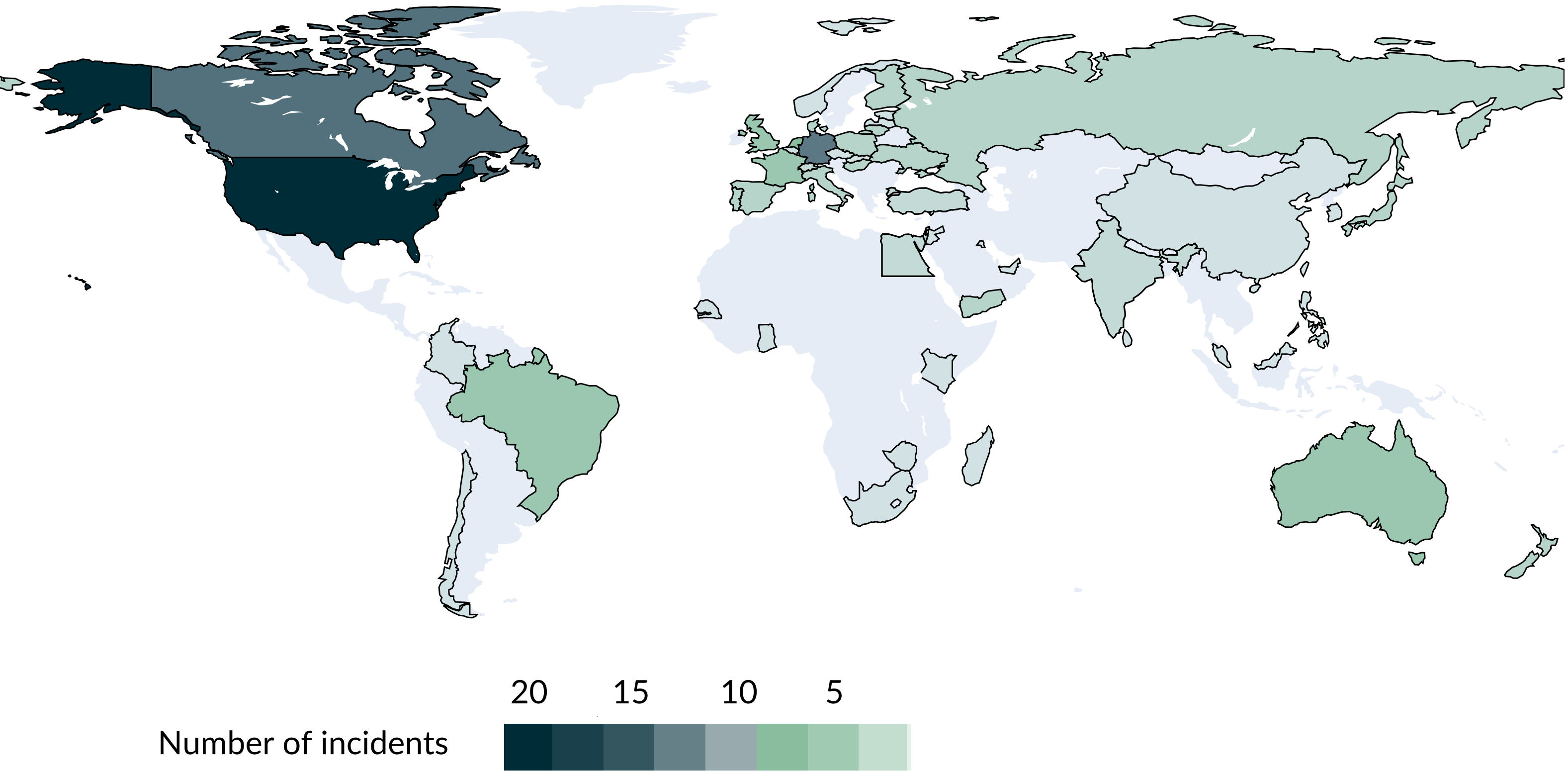
Disruptions of this kind may also be the results of ransomware attacks. In mid-September, the shutdown of data-dependent services of several government authorities in Colombia as a result of a ransomware incident led to interruptions in legal proceedings and interfered with the delivery of medical care.

The immediate target in this incident was the US-based telecommunications company IFX Networks - an Internet provider and the leading supplier of public-private cloud solutions in Latin America. In Colombia, the Ministry of Health and judicial bodies in particular were cut off from vital information flows due to their dependence on IFX data centres.

Restrictions as a result of the ransomware attack affected the ability to schedule medical appointments and access medical records. Delays in the processing of court proceedings also made it necessary to suspend trial deadlines for several weeks. According to the presidential advisor responsible for crisis management in Colombia, the responsible criminal group also gained access to the personal information of several million people.

The far-reaching disruptions highlight potential cluster risks that may be exacerbated by the concentrated use of individual cloud solutions if providers fail to take precautions.

Geographic distribution of operations



In total, the intrusion into the IFX data centres affected 619 organisations and over 6000 services, including services in Chile and Argentina. The Colombian Computer Security Incident Response Team's response centre responded to 35 requests for assistance, 20 of which were filed by companies and 15 by the public sector. In accounting for these events, the Colombian government is considering legal action and investigating whether the provider had complied with minimum cyber security requirements.

Focal points and targeting patterns

The most targeted sector in September 2023, as in the previous month, was critical infrastructure, with 50 cases (58% of new cases) recorded. This represents a 40% increase from the 36 cases in August.

The second most affected organisations were state institutions, with 42 cases (49% of cases recorded). This represents a significant increase of more than 60% compared to the 26 cases recorded in August. This increase is also noticeable in relation to previous months: while in previous months, around three out of every five cyber incidents affected critical infrastructure targets, state institutions had been targeted much less frequently, in only two out of every five incidents.

Looking at the countries affected, the United States continues to be the most affected, with 19 incidents. This is followed by Germany (11 incidents), a noticeable increase compared to the "quieter" summer months. Canada continued to be frequently affected, being targeted in eight incidents; the Netherlands had seven and Australia had five.

In contrast to the previous months, there was a noticeable shift in relative terms. The United States was only affected in 23% of all incidents instead of around 30%, while the number of incidents affecting EU member states remained at the 30% level observed last month, which still marks an increase from the month prior.

A look across the affected infrastructure sectors shows a combination of established and emerging trends: In July, EuRepoC for the first time registered the financial sector as the most affected infrastructure sector in the monthly review. This observation was repeated in September (eleven incidents). Five of the incidents affected crypto trading platforms, with services from China and Hong Kong (here and here), Canada, and the Seychelles being affected. Unlike many other cyber incidents in which the damage amounts are difficult to determine and tend to be based on averaged estimates, immediate losses are easier to estimate for crypto exchanges in light of the transparent documentation inherent to blockchain technology. Damages in September alone amount to over $240 million USD. In the financial sector, the theft of personal data from the savings bank subsidiary Deutsche Leasing was relevant for Germany.

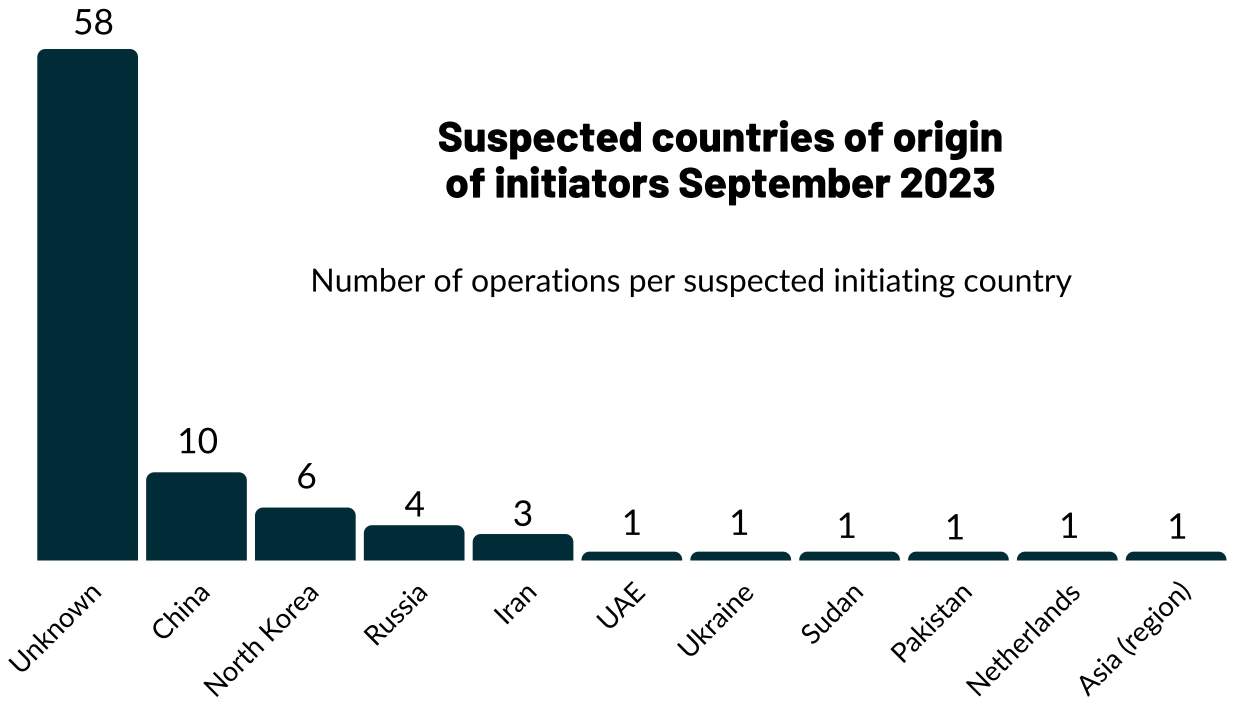
The healthcare sector continued to be frequently affected, with nine incidents recorded in September. The majority of these cases suggests no specific selection of targets, displaying spray-and-pray tactics. Other activities targeting the financial sector followed a similar pattern.

No homogenous picture emerged for the telecommunications sector, which was affected by nine incidents. Incidents comprised cyber espionage, such as the actions of the groups "BlackTech" against US and Japanese companies or those of "Sandman", while also including classic ransomware operations. The aforementioned effects of the ransomware attack against IFX Networks in Colombia exemplified the dangers that dependencies on central providers can pose to state institutions.

A review of targeted institutions highlights that the 27 incidents targeting sub-national authorities listed under “civil service/administration” represent the majority of incidents against public organisations; sub-national authorities accounted for almost two-thirds of these incidents. As in previous months, this may be attributed to the lower level of cybersecurity for local- and state-level authorities compared to national authorities. In Germany, these incidents included a DDoS attack on the website of the State of Berlin and incidents targeting educational institutions such as Furtwangen University and the Helmholtz Gymnasium in Zweibrücken. At a national level, the financial supervisory authority BaFin was affected by a DDoS attack, while an intrusion targeting the Federal Agency for Cartography and Geodesy in 2021 was only first publicly reported in September.

Threat actor profiles and attributions

In September, the percentage of cyber incidents not (yet) attributed to specific attacker countries (number: 58) levelled off around the 70% mark, at 67%. Non-state actors were held responsible in 27 of the 86 total cases recorded in September, which represents a percentage decrease of around 12% compared to August. Criminal actors were responsible in 20 of the 27 cases, with only one case involving a country of origin, Russia.



This emphasises the often transnational nature of increasingly professional hacker collectives and the difficulties in attributing potential links between these groups and specific countries. In each of the remaining seven cases, politically-motivated hacktivists claimed responsibility, with one country-of-origin attribution each to Ukraine, Russia, Pakistan, and Sudan. However, the latter attribution of a DDoS attack by Anonymous Sudan remains contested. The group had previously been described by threat intelligence companies as a false flag operation by the Russian group KillNet. In this case, the group claimed to have blocked access to the social media network X (formerly Twitter) for around two hours. According to the group, their goal was to persuade Elon Musk, the owner of X and CEO of SpaceX, to offer his Starlink satellite Internet service in Sudan in the future and to draw attention to the civil war situation on the ground.

Elon Musk's role as CEO of a company that enables countries to access the Internet independently, without needing undersea cables, therefore continues to wield considerable (geo-)political impact, beyond Ukraine.

Reports at the beginning of September revealed for the first time that Musk had deactivated coverage of Starlink in the area around Crimea, thwarting a surprise drone attack by the Ukrainian military a year earlier, as he feared that this could make him partly responsible for a further escalation of the war. Musk's company, SpaceX, had made its Starlink product available to Ukraine at its own expense and via an agreement with the US Agency for International Development (USAID), but not as part of a contract with the US Department of Defence. The increased importance of the private sector in armed conflicts is also reflected in the recommendations recently published by the International Committee of the Red Cross for technology companies on how they can protect civilians from digital threats.

Cyber proxies were named as responsible actors in 17 of the 86 total cases in September, which is roughly 6% more than in August. Of these 17 cases, seven were attributed to China, six to North Korea, three to Iran, and one to the United Arab Emirates.

China was also the point of origin for the most proxy operations in August. In September, the country also topped the overall list of attributed attacker countries of origin, with ten total incidents, placing it ahead of North Korea, Russia, and Iran. This group of four has consistently ranked at the top, although the respective positioning varies over time. In the case of North Korea, the six proxy operations recorded reflect the primary motives of the regime in Pyongyang for carrying out cyber operations: four of them focussed on data theft from the arms industry (including in Germany and Israel) and research organisations (e.g., against an aerospace research institute in Russia). Activities in this vein presumably are designed to further strengthen North Korea's own nuclear weapons programme and bolster its deterrence capabilities. The remaining two cases targeted the financial and cryptocurrency sectors, in suppport of regime resources under existing international sanctions. Cyber operations can give digitally-isolated countries such as North Korea an asymmetric advantage by turning the existing interdependencies of democratic countries in cyberspace into vulnerabilities.

In the case of China, four of the seven proxy operations stand out as compromises of state entities within its immediate neighbourhood, with the presumed aim of cyber espionage. Even though the People's Liberation Army (PLA) has developed stronger capabilities for military-oriented cyber operations in recent years in the context of geopolitical stand-offs with India or states bordering the South China Sea (see the recently-published annual report of the US Department of Defence), the focus remains on data theft. Targeting concentrates on intellectual property or state secrets, while also extending to collecting date on regime opponents.

The number of operations linked to Russia's war against Ukraine fell slightly compared to previous months (3 operations), but the presence of the hacktivist group NoName057(16), which was responsible for two of them, remained constant.

Threat intelligence reporting in September addressed several previously unknown groups. SentinelOne and QGroup published a joint report on a previously undocumented "activity cluster" tracked as "Sandman." The group had spied on telecommunications providers in Europe, South Asia, and the Middle East in August 2023. Sandman activity may be tied to a private contractor, as no links to a specific state have been observed. It is conceivable that future operations by the group will provide additional evidence as to whether the group may have close ties to a state, and, if so, to which state the group may be sponsored or controlled by.

The Japanese threat intelligence company TrendMicro for the first time publicly detailed activities of the group "Earth Estries" in September, which has been operating since 2020. The group has been tracked spying on governments and technology companies in countries including Germany, Taiwan, the Philippines, Malaysia, South Africa, and the USA since at least early 2023 leveraging the Zingdoor backdoor, the TrillClient information stealer, and the HemiGate backdoor. According to TrendMicro, the observed tools, techniques, and procedures (TTPs) overlap with the FamousSparrow group, which has been active since at least 2019 according to threat intelligence company ESET.

With Bermuda, September saw a rarely-discussed state engage in attribution. On 21 September, Bermudian Prime Minister E. David Burt announced in a press conference that threat actors suspected of operating from Russia had paralysed large parts of the state's IT infrastructure. In public remarks addressing the incident on the followign day, Deputy Prime Minister Walter Roban emphasised the administration's efforts to limit the consequences of the incident and assured the public that no central emergency services were affected (e.g., 9-1-1). In September, Bermuda faces peak hurricane season, assigning particular importance to the undisturbed functioning of and public confidence in these communication systems. The Bermudian government's response to the incident was notably proactive and timely, even as no further details of the attribution to Russia have yet been released.

More from EuRepoC

In an SWP podcast published at the end of September, Annegret Bendiek and Jakob Bund discuss the increasingly sophisticated methods used by attackers in cyberspace and how political decisionmakers can respond most effectively.

In a new issue of the EuRepoC publication series "Major Cyber Incidents" (MACIs), the EuRepoC team discusses the KA-SAT 9A attack – the most disruptive wiper attack to date in the context of Russia's war against Ukraine – which also led to disruptions of companies in Germany.

Through the redesigned EuRepoC website, the Repository now provides an extended interactive version of the EU Media Reporting Tracker, which includes monthly-updated data on media coverage of cyber incidents in the EU.

In addition, 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