European
Repository of
Cyber Incidents

EuRepoC
Cyber Conflict Briefing

August 2023

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

Overall observations

In **August 2023**, 63 cyber operations were recorded in the EuRepoC database. This is a 26% increase from the previous month, and 7 operations more than the overall average recorded activity of 56 cyber operations per month.

The **average intensity** of operations recorded in August 2023 is 2.81, which is above the historical average (2.6). The striking increase in operations since February 2023 is partly explained by the fact that, since March 2023, EuRepoC has been recording all cyber attacks 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

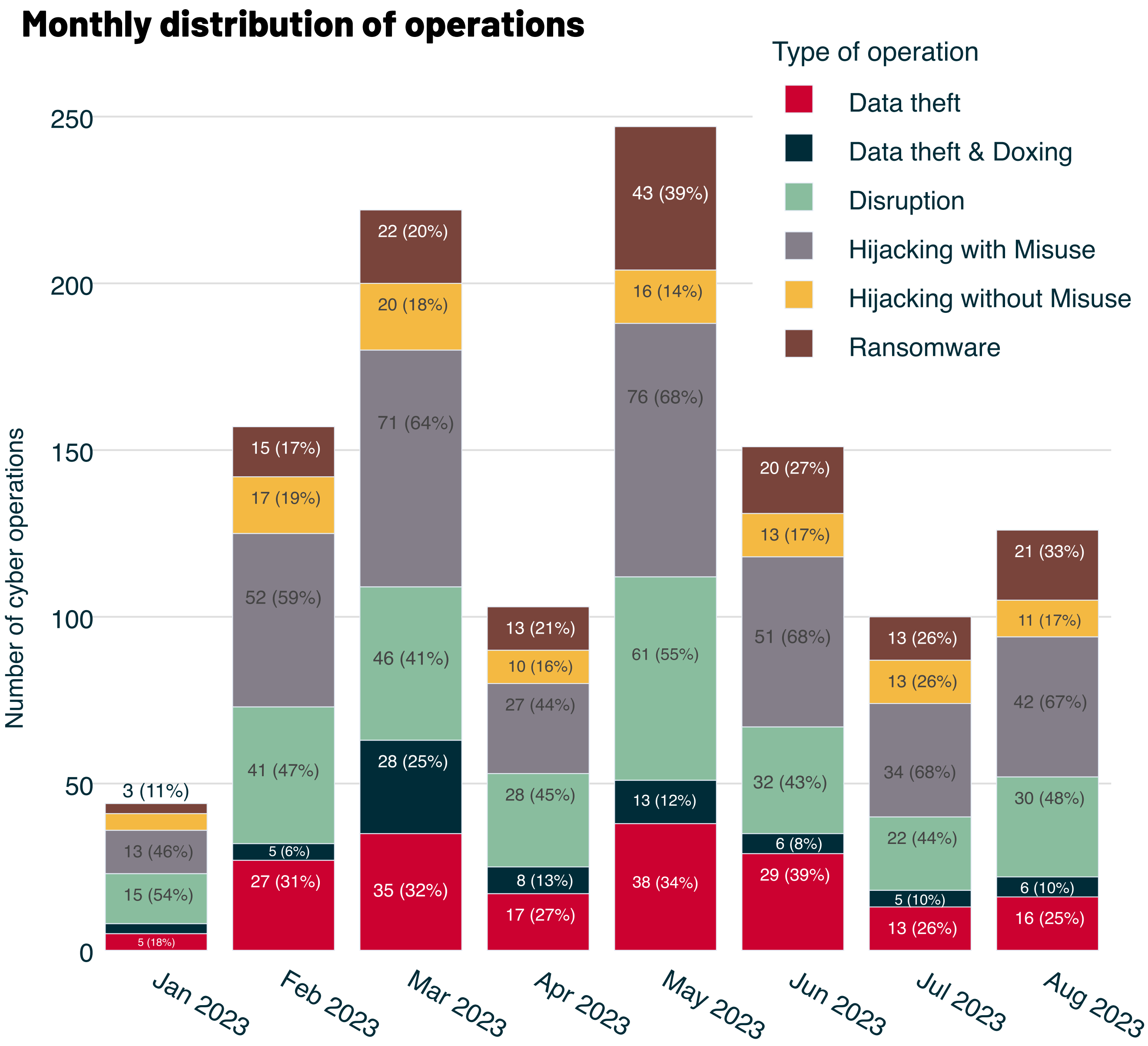
The Cyber Conflict Briefing is an analytic product prepared by EuRepoC. The German edition is published in collaboration with the **Tagesspiegel Cybersecurity Background,** accessible here.
It summarises the key trends, dynamics, and findings on cyber incidents as recorded by EuRepoC in a given month. These do not necessarily have to have taken place in August, 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 August 2023 are distributed across the following **operation types**:



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

The largest share of activity tracked in August comprises **"hijacking with misuse"** operations (67%). 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 attacker intent and, if applicable, identifies data theft or operational disruptions.

For example, in late August, the Greater London Metropolitan Police acknowledged that personal information of police officers and other employees had been stolen from a third-party service provider responsible for making badges. The police department, also known as Scotland Yard, informed all 47,000 employees of the possible theft of photographs, names, and other internal identification information. Undercover officers and investigators were then pulled from their assignments as a precautionary measure. On 14 September, the Manchester Police Department announced that the data of more than 12,000 employees, including 8,000 police officers, was also affected by the ransomware attack.

The incident underscores the importance of minimising the disclosure of data to only absolutely necessary information, especially when disclosing data to external service providers, in order to avoid the risk of misuse in the event of a data breach. In this case, the data leak did not affect any private addresses. The risk that the identities of security personnel could be disclosed also indicates a possible intersection between financially-motivated doxxing by criminal groups and disinformation attempts.

It is conceivable, for example, that ransomware actors are being used by the state, or working out of pure opportunism for their own benefit, to circulate information as part of disinformation campaigns to provoke hostility against law enforcement. Ideologically-motivated or terrorist groups could make use of this information to create so-called "kill lists" and incite violence against doxxed individuals.

The second most common type of operation recorded in August 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. We have recorded 30 such incidents in August.

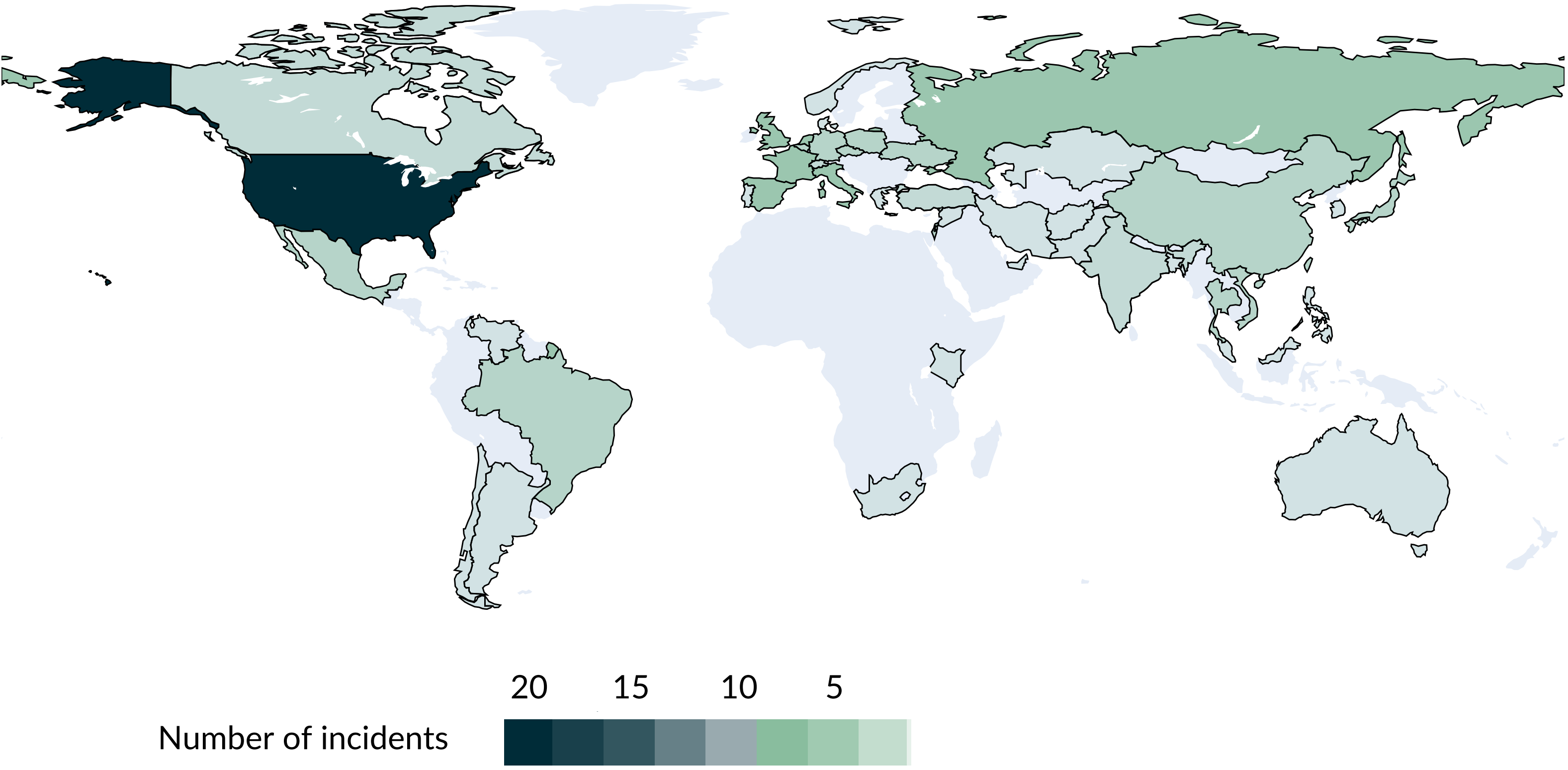
At the beginning of July, the port administration of Japan's largest cargo port, located in Nagoya, reported a ransomware attack. The resulting operational disruptions affected container logistics for several days. Limited ability to load and unload vans caused delays in goods clearance at the port, which also serves as a hub for automotive manufacturer Toyota to distribute components in its just-in-time production.

Initially attributed to the ransomware group LockBit, senior Japanese government officials in August expressed suspicion that state-directed Chinese actors could have been responsible for the attack. LockBit itself operates a ransomware-as-a-service model, granting access to its attack tools in exchange for payment or a share of any extortion money obtained. After a former programmer of the group leaked the basic building blocks of LockBit in September 2022, it became possible for actors without a connection to LockBit to carry out ransomware operations using similar methods.

If the suspicions of involvement by Chinese groups are confirmed, China would be following in the footsteps of other state actors in its attempt to conceal its own responsibility through the use of criminal elements.

In 2017, North Korea and Russia caused unprecedented economic damage through the uncontrolled spread of ransomware with WannaCry and NotPetya. In the past, state actors have also used ransomware to cover up other previously-executed actions and to hide the actual goal of an operation by wiping out or encrypting network and log data. Disguising the attack as the work of LockBit, if applicable in the case of Nagoya, would not only be an attempt to camouflage sabotage operations by portraying them as financially-motivated criminal activities, but would further be a false flag operation that draws attention to a specific other group. In light of international efforts, such as the International Counter Ransomware Initiative, to take disruptive action against ransomware groups and other criminal networks, such attempts to deflect blame may be associated with new risks of escalation.

Geographic distribution of operations



Focal points and targeting patterns

The most targeted sector in August 2023, as in the previous month, was critical infrastructure, with 36 cases (57% of new cases) recorded. This represents a slight increase compared to the 31 cases in July, but is relatively the same percentage of total incidents as in June and July. State institutions were the second most affected, with 26 cases (41% of cases). Here too, there was an increase (roughly 37%) from the previous month, and on a relative basis, this is close to the 40% of cases within the previous months.

A similar picture emerges when looking at the states affected: once again, the United States remains most affected, accounting for roughly one-third of the incidents (22 in total), which we attribute to its technological and industrial dominance in cyberspace.

EU member states were affected in 20 cases (32%), which is an increase from previous months in which the proportion was 20-25%. This month, Italy was the most affected EU state, with six cases; it was followed by France with four cases, while Spain and the Netherlands each had three. Germany was affected in two incidents and thus, as was the case last month, was underrepresented.

For the incidents targeting critical infrastructure companies that were included in the dataset, it can be seen that the healthcare sector was the most frequently affected sector with 10 incidents. Several hospital operators in the USA were affected (e.g., here and here), but so, too, were those in Portugal and Belgium.

For the financial sector, six new incidents were registered for August; half of the cases were "thefts" from cryptocurrency exchange operators (here, here, and here).

Six incidents were in the transport sector, of which two-thirds were short-lived DDoS attacks by pro-Russian groups on targets in EU member states (see below for more details). In contrast, the ransomware incidents attributed to the groups “Akira” and “Play” against Belt Railway Company of Chicago and several unspecified managed service providers are considered much more serious.

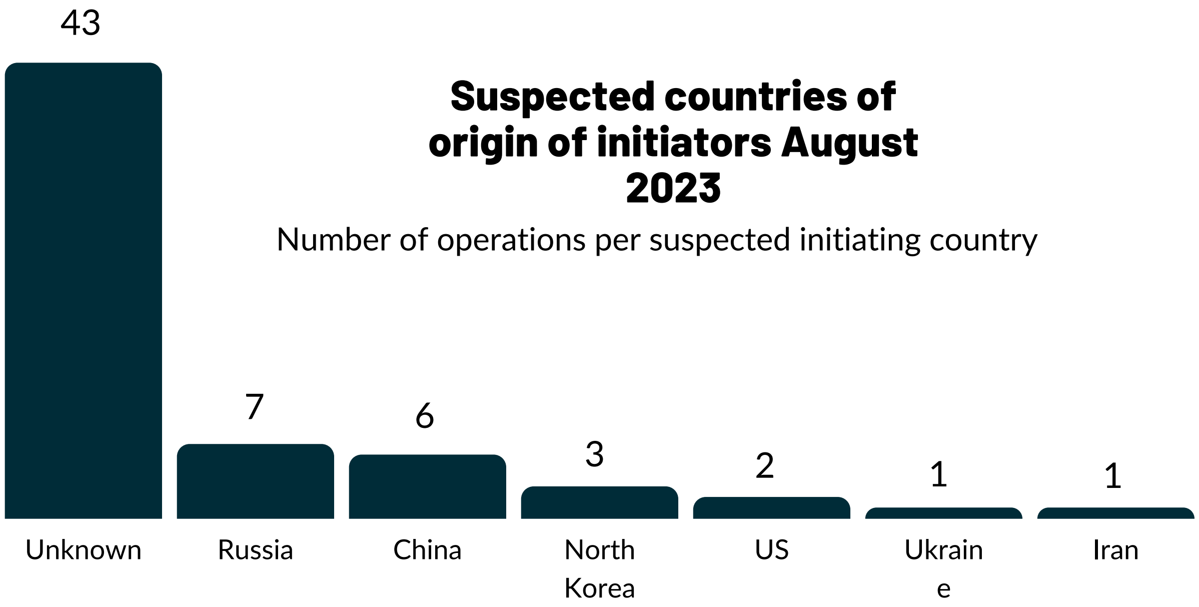
In the case of state institutions, local or regional authorities were once again more vulnerable than state-level targets. Among these, a total of ten educational institutions stands out. The variance of incidents within state institutions — from ransomware incidents at US and Swiss institutions, to a case of "CEO fraud" with damages in the millions of euros, to unauthorised access to email accounts at Heinrich Heine University in Düsseldorf — reinforces the impression that attackers act according to the "spray-and-pray" principle: they attack a large number of victims and have more success with local authorities that are less well-equipped in terms of IT security (see our Briefing from the previous month).

On a global level, three incidents attracted particular attention: it became known that both the Japanese National center of Incident readiness and Strategy for Cybersecurity (NISC) and Ministry of Defence networks were suspected of being spied on by Chinese state or state-backed actors (more on the latter incident below). In addition, it became known that unknown attackers had managed to penetrate the systems of the UK's electoral authority in August 2021, which was only noticed a year after the attack, in October 2022. Although mostly only publicly-known data was stolen, there have been warnings about further malicious use of the data, e.g., for targeted disinformation campaigns in connection with elections.

In addition to the unauthorised access to the email accounts of the University of Düsseldorf as mentioned before, the two incidents with German victims included a hack against the exiled Iranian Mansour Sohrabi, for which the Iranian-backed group "Charming Kitten" is held responsible.

Threat actor profiles and attributions

In August, the percentage of cyber incidents that were not (yet) attributed to specific attacker countries also settled around the 70% mark, at 68% (43 cases). In 27 of the 63 total cases, non-state actors were held responsible, which is a slight percentage increase of about 5% compared to July. Of these 27 incidents, 16 were attributed to criminally-motivated actors, while the remaining 11 were attributed to ideologically/politically motivated hacktivists. Seven of the 11 hacktivist operations reveal Russian involvement in the context of the war against Ukraine, which underscores its strong presence at the cyber level even 18 months after the war began. Responsible for all seven cases was NoName057(16), the most active pro-Russian hacker group besides KillNet since the onset of hostilities in February 2022. Eight of the 13 cyber incidents attributed to specific conventional conflicts in August revolved around the war against Ukraine. EU member states supporting Ukraine continue to be particularly caught in the crossfire of hacktivist operations, which targeted Czech, Spanish, Dutch, and Italian targets in August (all seven of the NoName057(16) operations).



Suspected countries of origin of initiators August 2023

Number of operations per suspected initiating country

The number of incidents attributed to so-called "cyber proxies" in our database in August was 9, with five of these incidents being attributed to Chinese attackers. Accordingly, China ranks only slightly behind Russia in the list of attributed attacker countries of origin in August, with North Korea following in next place, as was the case in July.

The two incidents attributed to the USA are striking, as US cyber operations are rarely publicised in terms of their presumed number. However, the two cases reflect two significant aspects; on the one hand, there is still a high danger of so-called "insider threats," and on the other hand, there is an increasing proactivity from law enforcement agencies when it comes to the operational shutdown/disruption of hacking networks/infrastructures. For example, it was revealed that an engineer at Arnold Air Force Base in Tennessee (USA) had taken home hardware and had allegedly gained access to communications of the FBI and various Tennessee state agencies. In mid-June, a member of the Massachusetts Air National Guard was indicted for publishing sensitive Pentagon information on his private Discord server, including explosive information on the US military's assessment of the outcome of the war in Ukraine.

These examples show that, especially in highly sensitive areas and in line with the increasingly-propagated "zero-trust" approach, it should not only be assumed that external actors have already gained access to one's own networks, but that one's own employees could also become a potential security problem. The second case with US authorship, on the other hand, demonstrates the increasingly-applied approach of "active cyber defence" on the part of state law enforcement agencies, as is currently also being discussed for the EU: as in other cases before, numerous law enforcement agencies, under the leadership of the FBI and with the participation of the German Federal Criminal Police, had rendered the so-called "Qakbot" botnet/malware harmless. According to the FBI, Qakbot had existed since 2008 and had since been used worldwide for ransomware and other cybercrime activities. In the coordinated law enforcement operation, the FBI gained access to the Qakbot infrastructure, redirected its traffic, and was ultimately able to disconnect it from the rest of the botnet by installing an "uninstaller" file on the infected computers and further preventing the installation of more malware.

From a technical point of view, however, this is not to be seen as cleaning the already-infected computers from potential other malware; it only means that their ties to the Qakbot botnet were broken. The case demonstrates the growing desire for international coordination between law enforcement agencies to counter cybercrime groups more widely and effectively, and to drive up the cost of conducting their operations to the point where their business model is no longer viable in the long run. However, law enforcement operations that require access to the systems of the cybercrime groups' victims pose an even greater challenge from a legal perspective than operations that only require access to the attackers' infrastructures, such as in the case of the concerted action against the ransomware group Hive that became public earlier this year. For all such operations, however, questions remain regarding long-term effectiveness without simultaneous imprisonment of the responsible persons behind the technology, since, for example, the Emotet malware was also ultimately detected again only a short time after a successful law enforcement operation against it in early 2021.

In four of the 38 cases in which a specific attributed actor could be identified, these were attributed by US authorities. The FBI attributed two, the NSA attributed one, and the US Department of Justice attributed one. Even though these numbers seem significantly lower than the number of incidents attributed by threat intelligence companies (12 in August), it is worth taking a closer look at the cases: the two FBI attributions (the self-attribution of the Qakbot shutdown and the attribution of a Lazarus campaign) were both published in the form of political statements on the authorities' websites.

A political attribution that is made through official channels is provided with stronger "weight"/formality. At the same time, however, it also places different expectations on the attributing government in terms of possible follow-up actions than in the case of "informal" attributions, such as the NSA's attribution of Chinese hacking operations against Japanese targets through a Washington Post article on 7 August. This type of attribution can have different motivations. In this case, it could be a deliberate attempt to put even more public pressure on an allied state to protect its own, and potentially US, systems more effectively in cyberspace without having to go through an official route. Without shared ideas or rules about when, how, and why democratic governments make official attributions of cyber operations and in which cases, the exact motivations can only be speculated. This, however, makes it difficult for outsiders to assess the "success" of an attribution without knowledge of the intended goal.

More from EuRepoC

In a major redesign, EuRepoC has expanded the possibilities to explore cyber operations interactively. Since 27 September, our redesigned website provides access to customised features that allow for dynamic visualisations of trends in the cyber threat landscape.

In a discussion of the new German National Security Strategy, Annegret Bendiek and Jakob Bund point out the need to include parliamentary oversight from the outset when considering cyber defence. As their commentary points out, a prerequisite for examining the suitability of proposed measures is also a prior determination of the structural characteristics of cyber threats.

In a new APT profile, Kerstin Zettl-Schabath, Benjamin Butz, and Camille Borrett deal with the Chinese group APT3/Boyusec, which disguised itself as a private company and spied on industrial secrets on behalf of the Ministry of State Security. APT3 stood out for its cooperation with government agencies, through which the group allegedly gained access to information about newly-discovered vulnerabilities in victims' systems.

In addition, EuRepoC provides information about new cyber incidents added to the database with a daily curated Cyber Incident Tracker. You can subscribe to this 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