European Repository of Cyber Incidents

EuRepoC

Cyber Conflict Briefing

July 2023

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

Overall observations

In July 2023, 52 cyber operations were recorded in the EuRepoC database. This is a 31% decrease compared to the previous month and 1 operation less than the overall average recorded activity of 53 cyber operations per month. The current decrease may be primarily explained by the summer season, as government hackers and cybercriminals also go on vacation, so less activity is typically recorded in July and August.

The **average intensity** of operations recorded in July 2023 stood at 2.84, exceeding the historical average of 2.6. The striking increase in operations since February 2023 is partly explained by the fact that, from March 2023 onwards, EuRepoC records 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 July, but may have started earlier. The focus is on technical, political, and legal aspects.

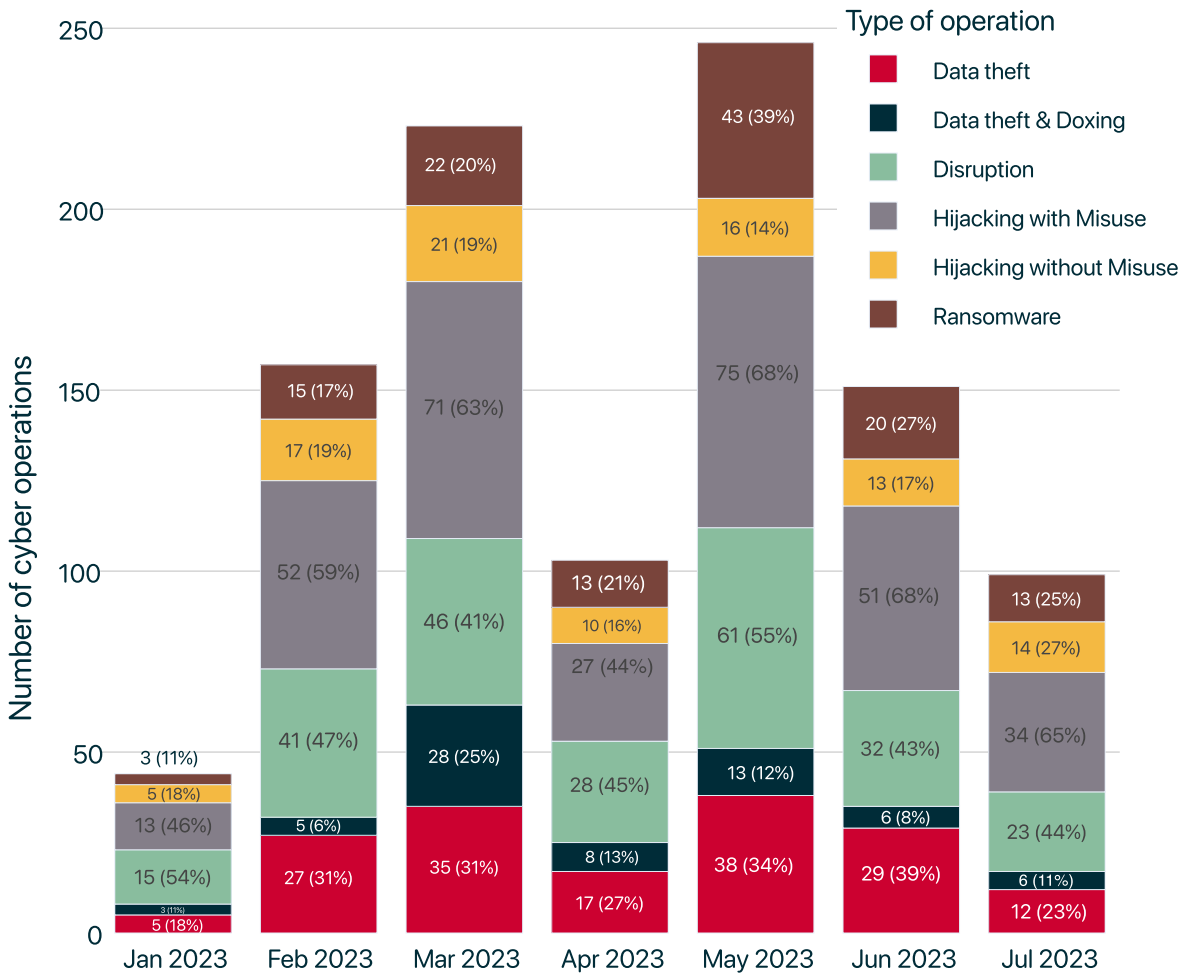
About EuRepoC

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 July 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 July comprises **"hijacking with misuse"** operations (65%). 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.

Of particular importance was a mid-July Chinese espionage campaign by the Storm-0558 group that stole at least several hundred thousand government messages, as admitted by Microsoft and according to media reports in the United States. Headlines stated that email accounts of the US Secretary of Commerce, the US Ambassador to China, and the State Department's Subdivision Chief for East Asia were also affected. Initial analysis by Microsoft indicated that Storm-0558 had also focused on European targets in previous espionage attempts.

In the meantime, further investigation by independent security firms, including cloud security firm Wiz, identified a much broader potential threat.

Storm-0558 gained access to Microsoft-managed email accounts using a stolen Microsoft Account (MSA) signing key, a service used to verify access privileges. Using the key, the threat actors were able to independently create access tokens that granted unrestricted access even to accounts with multi-factor authentication enabled. Although the key was actually designed for consumer accounts, a flaw in the validation process also allowed tokens to be made for the Azure Active Directory (Azure AD) identity service, which is aimed at business clients. Microsoft itself promotes Azure AD as access protection "to fend off 99.9 percent of cybersecurity attacks." Attackers also reached employee accounts belonging to government agencies this way. Furthermore, through this connection to Azure AD, the stolen key could be used to generate access tokens for a variety of other Microsoft cloud services. To counter exploitation, Microsoft locked down the affected key and revoked associated tokens. Newly created keys are now stored for consumer accounts in a strengthened, secure hardware environment.

According to Wiz's findings, applications that confirm access privileges using locally-stored credentials could still be vulnerable to the counterfeit tokens. Because logs were only available in certain payment models leading up to the case, it is sometimes impossible for app developers to track any compromise. Microsoft has since announced that it will make access logs freely available. However, this change cannot provide any information retroactively. The full extent is therefore virtually impossible to grasp in terms of its impact.

The measures taken after the case became known are limited in their protective capabilities in two respects. First, threat actors may have set up backdoors in the target environments and, to that extent, made themselves independent of the compromised and now-blocked key. Second, as security researcher and former NSA employee Jake Williams notes, the disclosure of the compromise influences the attackers' operational logic. Storm-0558's initial selective targeting was motivated by the desire to remain undetected for as long as possible. The exposure of the espionage campaign leads to a reversal of this incentive structure, according to which the maximum possible exploitation of applications that are currently still vulnerable via the "Log in with Microsoft" feature becomes more important.

On August 11, the US Secretary of Homeland Security announced that the Cyber Safety Review Board, in only its third investigation to date, will look into the case and develop recommendations.

"Disruption" operations accounted for the second-most common type of operation recorded in July. These are operations aimed at putting an information technology service out of operation. A disruption operation thus affects its availability. The majority of disruption operations are typically temporary in effect. In July, EuRepoC recorded 23 such operations.

Sustained high levels of ransomware activity continue to define the pattern of disruptive operations, although according to studies by forensics firm Coveware, the percentage of affected organisations that met ransomware demands reached a low of 34% in the second quarter of 2023. Four years ago, that figure was nearly 80%.

This decline is put into perspective in part by a massive increase in the amount of ransom payments made. In the second quarter, the average amount of these payments was more than $740,000 - a 126% increase from the previous quarter.

Bangladesh Agricultural Bank (BKB) was the target of such an extortion attempt, as the ransomware group responsible, AlphV/BlackCat, announced on 7 July. Representatives of the bank had previously confirmed that hackers had gained access to its servers. Bangladeshi media reported problems accessing software systems, citing information from bank employees. According to the bank's assessments, there was no leakage of data or disruption of customer services as part of the incident. Later statements by the bank's executive director attempted to put the events in a different context, denying that a hack had occurred and instead blaming server maintenance for the incident.

These post-incident statements differ from earlier statements by the bank that external disruptions had also temporarily affected bank transactions. However, the case also shows that, in addition to transparency and reliability, public communications from ransomware victims must also be prepared for attempts by ransomware actors to interfere.

For example, the bank's statements stood directly in contrast to actions claimed by AlphV/BlackCat: after the bank decided against negotiating with the group, AlphV/BlackCat began releasing allegedly stolen data and casting doubt on the bank's previous statements about the nature and extent of the incident. Threatening to escalate matters further, the group announced its intention to contact BKB customers directly with captured contact information.

AlphV/BlackCat held out the prospect of persuading customers to withdraw their deposits in a fictitious warning about the bank's impending insolvency. In such a critical and concentrated mass, these potential capital withdrawals could also develop the possibility of a bank run.

Averting such a scenario also depends in significant part on the affected company's trust relationship with its own customers - a variable in incident response plans that companies typically have more control over.

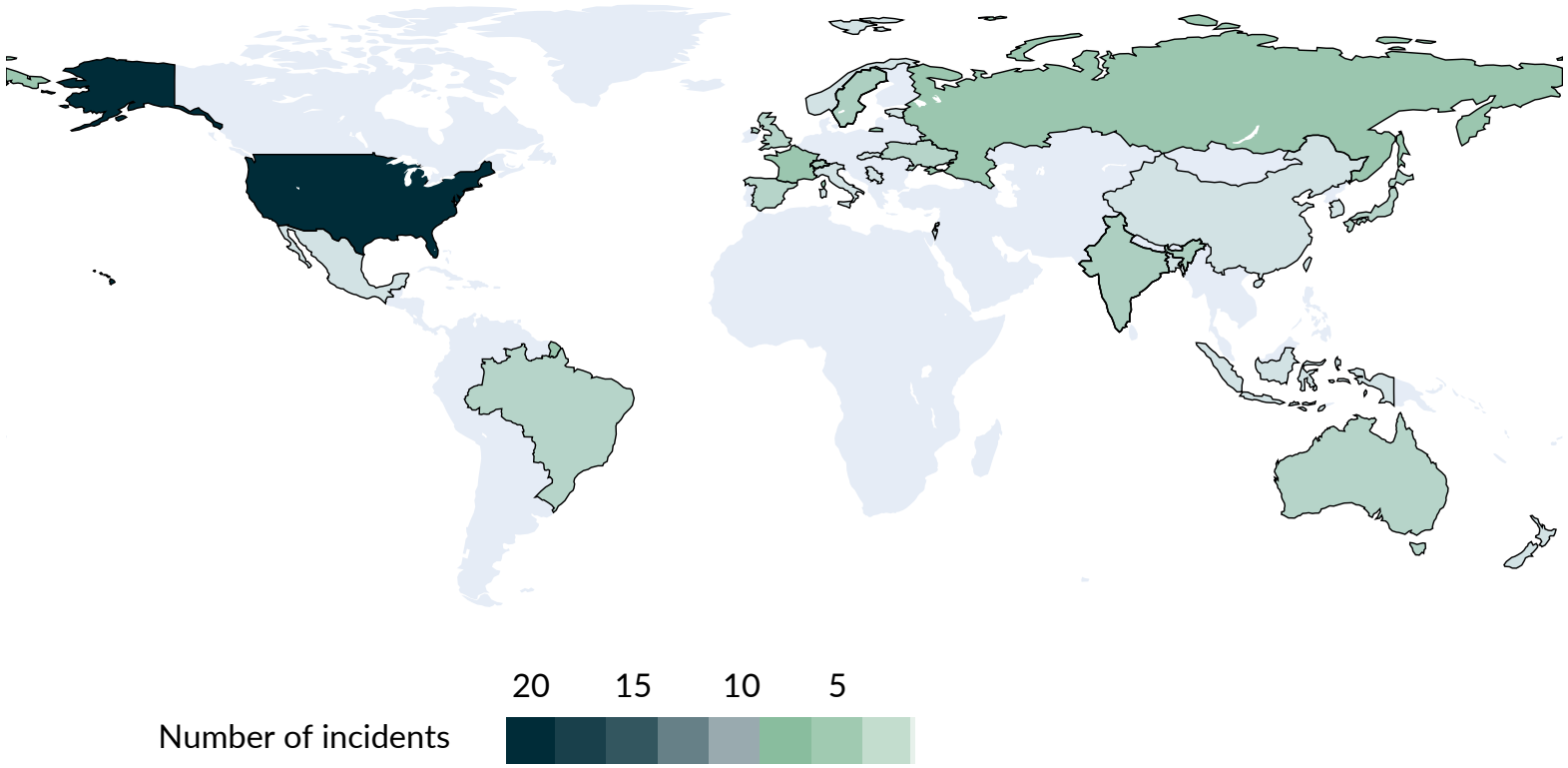
AlphV/BlackCat also made an "application programming interface" (API) for its extortion website available to the wider public in July, presumably to put even more pressure on victims who had recently refrained from paying ransoms, such as US cosmetics company Estée Lauder.

Past actions by the gang, which emerged as a spin-off of the DarkSide ransomware group responsible for the attack on Colonial Pipeline, show that members are also willing to take actions that cause longer-term economic damage.

Focal points and targeting patterns

The most frequently targeted sector in July 2023, as in the previous month, was critical infrastructure, with 31 cases (62%) of the new cases recorded. This represents a decrease of about one-third from the amount of critical infrastructure cases in the previous month (45 cases), but makes up roughly the same percentage of total attacks as in the previous month (60%). Government institutions were the second most affected, with 19 cases (38%); here, in line with the overall summer sink, there was a 42% decrease.

Geographic distribution of operations



The United States remains the most affected by cyber incidents, due to its technical and industrial exposure: 18 incidents were recorded against the US in July, roughly following the pattern in previous months, in which such cases made up about one-third of all attacks. European countries were targeted in cyber incidents a total of 20 times (nearly 40%). Of these, slightly more than half were EU member states (10 cases), with France being the most affected EU country this month, with four incidents. Among non-EU states, incidents involved Russia (4), the United Kingdom (3), Ukraine (3), and Norway and Serbia (one incident each). For Germany, no incidents were included in the database in July, which is a noteworthy change compared to previous months.

Within critical infrastructure targets, another outlier emerges for July compared to previous months: with just under a fifth of the total incidents (9), the financial sector was the most frequently affected industry. Most cases concerned "thefts" on cryptocurrency exchanges, in some cases with considerable amounts of damage that became publicly known, such as an attack on CoinsPad (from Estonia), with reported damage amounting to $37.3 million USD. The sum was somewhat lower in a case at Poly Network, which had already been affected in 2021. Despite these crypto attacks, traditional financial businesses did not remain unaffected: last year saw the theft of over $20 million USD from the British neobank Revolut, which has only now become public.

Among incidents involving critical infrastructure targets, the healthcare sector continues to be frequently affected, with nine cases recorded in July - a relative parallel to the previous months. Almost half of the cases in July involved ransomware incidents, and two-thirds (also) involved data theft, which could almost always be classified as sensitive.

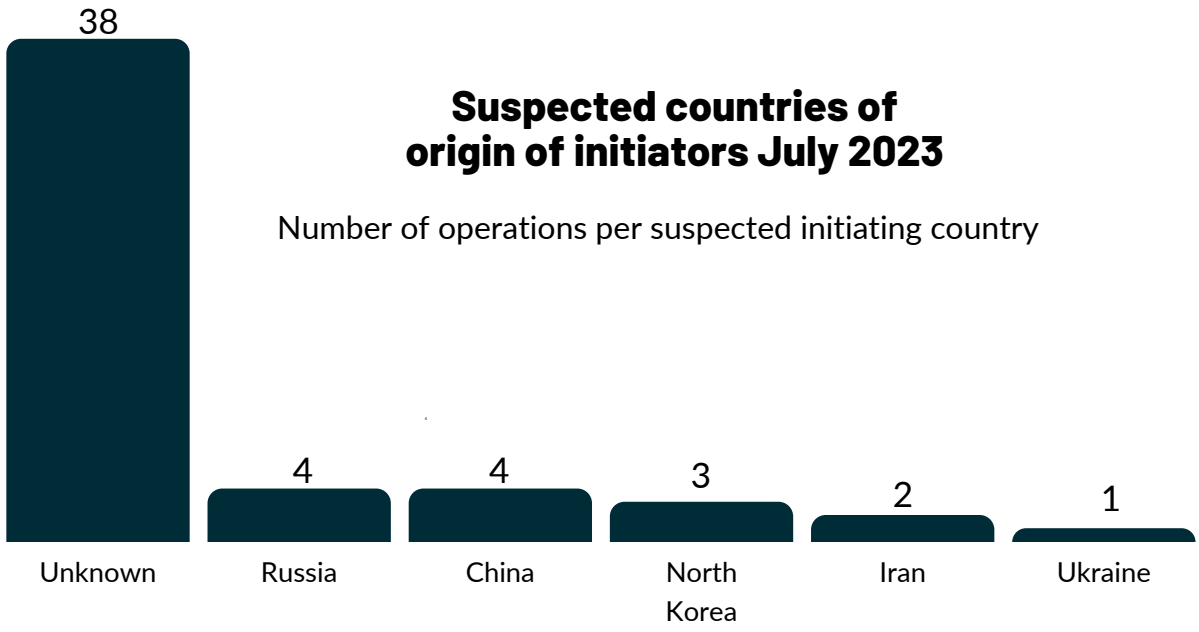
In the case of government institutions, a high number of operations targeting regional and local authorities can be seen with eleven cases, such as two of the four incidents affecting France. As mentioned in the May briefing, regional and/or local authorities often have a lower level of IT security than national authorities, for which a total of seven cases were recorded in July. Regional/local authorities could therefore also fall victim to so-called "spray-and-pray" operations in particular, in which no specific authorities are targeted, but the success of the operation results from the high number of infection attempts against a broad mass of organisations.

Threat actor profiles and attributions

In July, the percentage of total cyber incidents not yet attributed to specific attacker countries leveled off at 73% of the recorded operations, or 38 yet-unattributed operations. In 20 of the 52 total cases in July, non-state actors were held responsible, which, at 38%, is only one percent less than in the previous month of June. So-called "cyber proxies," i.e., state-sponsored and/or contracted hacking groups, were identified as perpetrators in eight incidents. As in June, Russian cyber attackers ranked second most-active in July, together with Chinese groups.

What is striking in July is the far lower diversity of countries of origin of the attackers. Apart from the "usual four suspects" - Russia, China, Iran and North Korea - only Ukraine appears in the list. As previously discussed for the generally significantly lower number of cases in July, the "summer break" of offensive actors in cyberspace can also be responsible for this, at least in part. This could be especially relevant for countries that already have a lower level of activity during the rest of the year compared to the four countries mentioned above, which could thus have led to a complete absence in recorded incidents for such countries. Actors from Russia, China, Iran, and North Korea are instead offensively active in cyberspace in far greater numbers and frequency. These countries also have historically grown larger numbers of patriotic hacker groups as well as state-supported APTs, which is why, even if one group is temporarily inactive, incidents from these countries are still recorded during the summer months. However, also on the part of the targets and their IT departments, as well as the "defending" or investigative incident response/threat intelligence companies, the vacation period in July and August could lead to a lower capacity for detection, analysis, and public reporting of cyberattacks.

In seven of the eight incidents in which cyber proxies were identified as responsible actors, a specific country was also named as the principal supporter. In the case of the 20 operations attributed to non-state attackers, a country of origin was only attributed six times.



Of the remaining 14 operations that were not attributed directly to a country, seven were ransomware operations, for which often no specific country can be attributed, for example because the grouping operates transnationally, like an internationally-operating cybercrime enterprise. The common denominator here is less patriotic/national motives, but rather the common pursuit of financial gain. However, this can also lead to disagreements and conflicts within a transnational cybercrime group in the event of a violent conflict, such as the Russian war against Ukraine; this was demonstrated by the so-called "Conti Leaks" last year. These led other groups to publicly pledge support neither to Ukraine nor to Russia, but instead to claim political neutrality for themselves so as not to jeopardise their own business model.

Furthermore, three of the 14 cases were attributed to the hacktivist group SiegedSec. According to public information, this group was formed in April 2022 and, according to its own statements, mostly carries out politically-motivated attacks. However, it sees itself more a "black hat" group than hacktivists, as its members are often simply interested in chaos and digital destruction. Such statements are often difficult to assess or even verify.

In one case in July, the group had stolen more than 700 internal documents from the NATO Community of Interest Cooperation Portal and published them via Telegram on 24 July. As per the group's own statements, this was not done in the context of Russia's war against Ukraine, but in response to alleged, unspecified "human rights abuses" by NATO countries. At this point, no further speculation can be made about the credibility of these statements, but what is striking so far is the grouping's strong focus on US targets, such as in two other cases added to the EuRepoC database in July. In the first case, the group allegedly targeted various US states because of their recent legislative initiatives to ban gender reassignment treatment for transgender youth and, according to the group, stole data and defaced their websites. In the second case, the group gained access to the systems of US technology company ITC Global and deleted customer accounts used to monitor satellite receivers. In addition, the group claimed to have "targeted" satellite receivers and Industrial Control Systems (ICSs) across multiple US states, again due to their proposed legislation to ban gender reassignment. However, whether and in what form the aforementioned targets were actually affected by cyber operations remained unclear.

The example of SiegedSec illustrates the extremely challenging attribution of attacker identities based on self-communicated motivations, as these can vary across cases or can be a mere pretext to disguise an actor's actual motivations. However, due to the often heterogeneous composition and membership structure of hacktivist groups, it is still possible in principle that their operations do not follow a stringent profile regarding target and motives over time.

The cyber operation against the Wuhan Earthquake Monitoring Centre, made public on 26 July by the Chinese newspaper *Global Times*, reflects the People's Republic of China's temporary "imitation" of public-private attribution practices of Western countries, some of which are cooperative or based on a division of labour. For example, according to the report, both the state-run Computer Virus Emergency Response Center and Chinese cybersecurity firm 360 Security Technology found an unspecified trojan in network technology used for seismic observations at the Centre. Initial investigations blamed state-sponsored attackers for the incident, according to the *Global Times*. Furthermore, the activity had been traced to US territory. Officially, this does not represent a direct-state attribution to the US because, from a technical perspective, the attack could have been carried out only from servers or computers in the US, but could have been initiated and controlled from another country. Nevertheless, this indirect attribution is likely to have been intended as a signal to the United States. Even though statements by the Chinese Ministry of Foreign Affairs spokeswoman are mentioned in the media report, accusing the USA of double standards and its own cyberattacks, among other things, it cannot be clearly confirmed that these reported statements referred to the present case in Wuhan.

The fact that other Russian companies besides Kaspersky and Group-IB have entered the "attribution business" is shown by a report from Positive Technologies. The company had been sanctioned by the US Treasury Department in April 2021 for providing computer network security solutions to Russia's domestic intelligence agency FSB, among others; it was also sanctioned by the EU on 23 June 2023, under Regulation No. 269/2014. In the 24 July report, the company makes public a cyber espionage operation by Chinese cyber criminals called "Space Pirates" against Russian and Serbian organisations.

More from EuRepoC

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

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

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

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