European
Repository of
Cyber Incidents

EuRepoC
Cyber Conflict Briefing

October 2023

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

Overall observations

In **October 2023**, 79 cyber operations were recorded in the EuRepoC database. This is an 8% decrease from the previous month, yet 21 operations more than the overall average recorded activity of 58 cyber operations per month.

The **average intensity** of operations recorded in October 2023 registered at 2.36, 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.

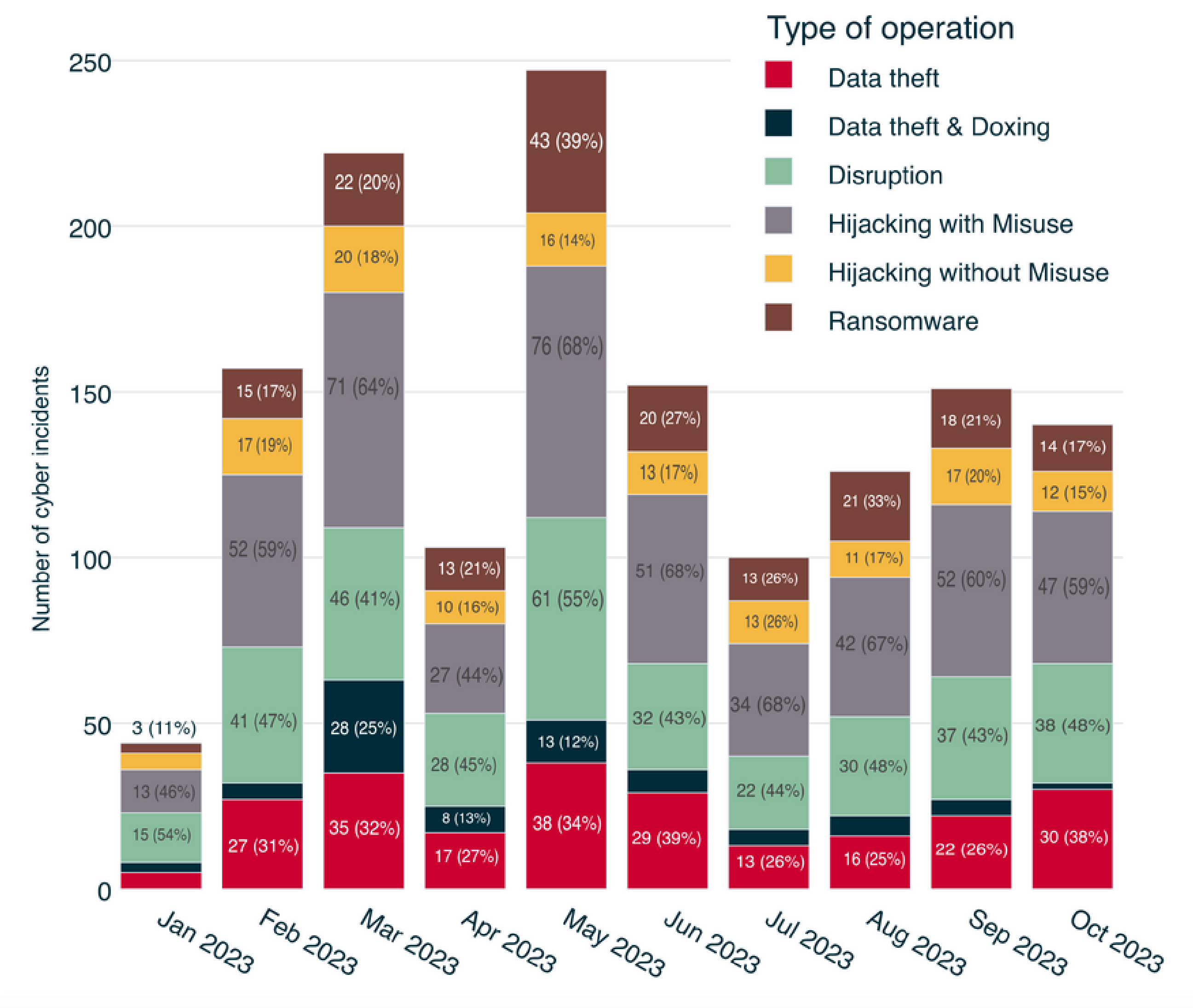
About EuRepoC

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 October 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 October comprises **"hijacking with misuse"** operations, with 47 cases (59%). 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.

Reporting by Kaspersky during October exemplified the challenges involved in discerning motives and the strategic classification of such operations. More than five years after the first discovery of an alleged cryptomining malware, findings by Kaspersky's security researchers point to its hidden espionage objectives. Code components of the StripedFly malware show parallels to tools used by the Equation Group, which is suspected to be operating under the US National Security Agency (NSA).

The initially-discovered cryptomining module was presumably intended to conceal other capabilities of greater strategic value to the operatives. Among others, the malware uses an exploit with marked similarities to EternalBlue, which takes advantage of a vulnerability in the SMBv1 network protocol to spread almost without restrain. According to Kaspersky's observations, elements of the exploit were last updated on 22 April 2023. Hidden modules are capable of credential theft, taking screenshots and audio recordings, and collecting extensive information about compromised systems.

The presumed importance of stealth to StripedFly also derives from special efforts to conceal the ties to the command-and-control server controlling these capabilities. To this end, StripedFly routes communication through a custom TOR client.

Kaspersky points out that StripedFly's use of EternalBlue was observed as early as 2016, more than a year before the Shadow Brokers group released the exploit on 14 April 2017. According to these findings, StripedFly experimented with disguising espionage operations as a cryptominer even before NotPetya attempted to disguise sabotage intentions as a ransomware attack in June 2017.

The second most common type of operation recorded in October comprises "disruption" operations (48%). Such activity refers to operations aimed at disabling an information technology service. Accordingly, disruptive operations affect the availability of data. Disruptions are generally temporary in nature. In the case of ransomware, however, blocked access to critical data can also cause outages over a longer period of time. EuRepoC recorded 38 disruption operations in October.

At the end of October, Microsoft documented several campaigns in which the criminal collective Octo Tempest increasingly focused on the use of encryption Trojans. Also known as 0ktapus, Scattered Spider, UNC3944, Starfraud, Scatter Swine, and Muddled Libra, the group had previously been known to sell Trojan access to criminal third parties for further exploitation.

The changes in Octo Tempest's activity profile observed since mid-2023 coincide with reports about its suspected collusion with the BlackCat/ALPHV ransomware group. In an indication of this collaboration, Octo Tempest has communicated threats to release stolen data via BlackCat's leak page and used the group's malware - primarily against targets in the hospitality, retail, manufacturing, financial, gaming, and technology industries.

BlackCat benefits from this alliance through the sophisticated social engineering techniques that are the hallmarks of Octo Tempest and have enabled the group to impersonate the employees of its targets' IT departments and help desk teams. These techniques have positioned the group to obtain credentials from actual employees or trick them into installing remote access tools. Upon gaining access, Octo Tempest members also covertly attend their victims' incident response meetings with the presumed intention of adapting their own approach to evade detection and secure their presence on the networks.

In a drastic escalation of the outfit’s social engineering methods, the group has in some cases attempted to obtain login data by threatening physical violence against employees and their relatives. The ability to convincingly deceive, which characterises Octo Tempest, presumably derives from the its large share of native English speakers.

Security analysts believe that the group includes members in the UK and the US. Against the background of this suspected composition of Octo Tempest, the cooperation with BlackCat as a Russian-speaking constellation appears to be an unusual combination. Operational links of this kind into the jurisdictions of victims, as seen from BackCat's view, are rare. Members operating from the US, for example, pose a risk to ransomware networks if accomplices are arrested by law enforcement and reveal internal details about their operating principles to authorities.

Historically, the use of BlackCat ransomware has focused heavily on organisations in the US. The vast majority of BlackCat's identified victims prior to September 2022 have been US-based targets (58.7%). There are indications that BlackCat, in line with this geographic focus, intends to use new reporting obligations by the US Securities and Exchange Commission, which will take effect for publicly traded companies from mid-December, as additional leverage to force ransom payments.

This operational footprint of BlackCat/ALPHV is consistent with Scattered Spider's strong geographic targeting preference for US-based organisations. Security analysts assume that BlackCat/ALPHV, which became active in November 2021, is a formation of developers recruited from the former line-up of Darkside. The now disbanded group was responsible for the Colonial Pipeline ransomware attack, which caused disruptions in fuel distribution in the US in May 2021. Darkside was also suspected of maintaining links to REvil. Several members of REvil were arrested by the FSB in Russia in early 2022. The White House believes that at least one of those arrested was involved in the attack on Colonial Pipeline.

In a request dated 16 November, the FBI and CISA asked for information about the group's communication methods and encryption techniques to develop an integrated understanding of Octo Tempest's activities and mainstream mitigation measures.

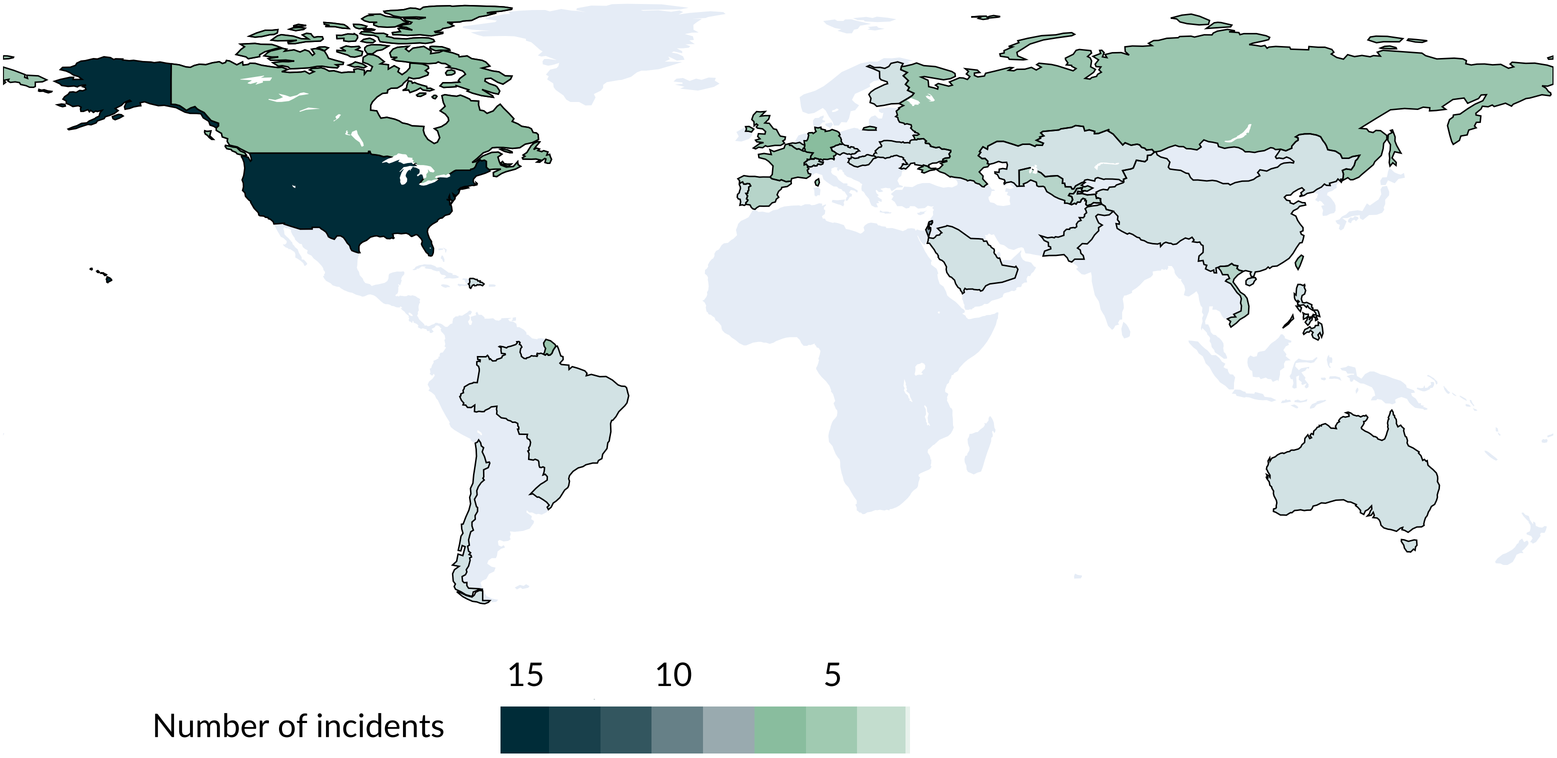
Focal points and targeting patterns

As in the previous month, the most frequently affected target sector in October 2023 was critical infrastructure, comprising 39 (49%) of the newly recorded incidents. This marks a decrease of 25% compared to the 50 cases of September, which is also reflected on a relative level - in the previous months, around three in five recorded incidents affected critical infrastructure.

The second-most affected sector were state institutions, which were targeted in 34 cases (43%). This also represents a decline, but remains roughly in line with previous months in relative terms.

Israel registered as a focal point of malicious cyber activity in October. While the US continues to be the most frequently affected country with 14 incidents (almost one fifth of all incidents) - in reflection of its attack surface and prominent role in technology supply chains - Israel has become the target of hacktivists in several instances following the Hamas attack on 7 October. With eight incidents that met the Repository's inclusion criteria, Israel recorded as the second-most affected country. Individual incidents and how they fit into the decades-long conflict are detailed in the threat actor and attribution section of this briefing.

Geographic distribution of operations



For the 16 cases involving EU member states EuRepoC recorded, Germany was the most frequently affected member state, with five incidents, and also ranked third worldwide. Germany was followed by the UK and Taiwan, each with four incidents, with the next most frequently targeted EU member state, France, affected in three incidents.

Of the critical infrastructure companies targeted, most incidents affected those in the telecommunications sector (nine cases). These included disruptive operations - some in apparent connection with the hostilities in the Middle East even as their immeediate targets are based in other geographies, including a DDoS attack on Brazilian Internet service providers. Other incidents showed no discernible link to geopolitical events, such as an incident at the British mobile phone provider LycaMobile. Two incidents related to the war against Ukraine.

Several incidents appear to be typical deployments of ransomware by cyber criminals, such as those affecting a Chilean telecommunications company and Südwestfalen-IT, an IT service provider for several dozen municipalities in Germany.

The healthcare and critical manufacturing sectors also remain frequently affected, with eight and six newly recorded incidents, respectively. The majority of attacks in the healthcare sector were of a disruptive nature, with the intensity ranging from several DDoS attacks on hospital websites in Israel (see below) and Canada, to operational disruptions at a Swiss psychiatric clinic and two hospitals in France. In similar incidents in the past, the use of ransomware - which, according to ENISA, poses the greatest threat to the healthcare sector - was often a contributing factor. In the specific cases tracked for October, the use of ransomware was at least not publicly reported.

For the critical manufacturing sector, theft of confidential data is the main focus, although the underlying motivation may still be to harness stolen data for the extortion of ransom payments, as observed for cases involving Octo Tempest or the US company BHI Energy. Instances in which the exfiltration of data appeared to be linked to industrial espionage objectives were reported in October for several companies in the defence sector, as well as companies in the semiconductor industry across Asia.

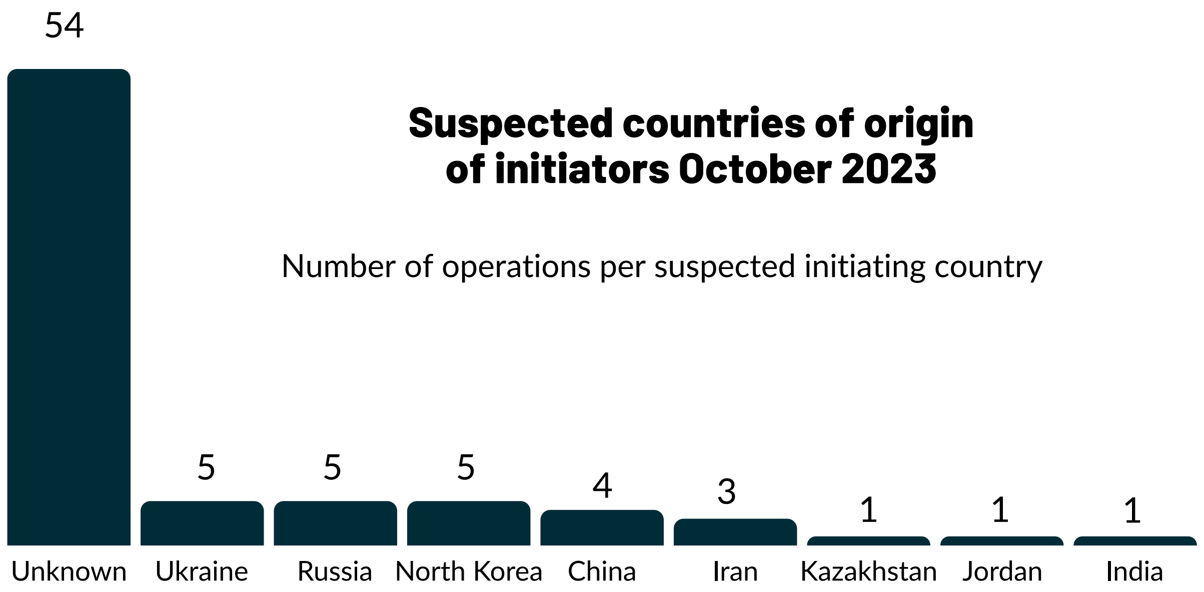
Of the cases affecting government institutions, half involved government entities and other institutions at the national level, while 14 new incidents, or 41% of all targeted government institutions, were directed against lower-level authorities. The consolidating pattern of increased severity of incidents targeting sub-national public institutions observed over the previous months extends to October. Incidents affecting government agencies in Australia, Belgium (here and here) and Czechia, for example, all fall into the "DDoS attacks" category. By contrast, countries outside Europe and North America whose cyber defences are perceived to be weaker - e.g., Guyana, Mongolia, and countries in Central Asia - were affected by serious data thefts, in some instances also involving ransomware. Similar observations emerged for public institutions at the sub-national level: In Germany, for example, the Hanover University of Applied Sciences and Arts and the municipality of Grasellenbach were targeted. The most recent activities affecting German organisations were DDoS attacks against the websites of several municipalities in mid-October.

Threat actor profiles and attributions

In October, the majority of cyber operations recorded could not (yet) be attributed to a responsible party. In 67 % of cases (54), the responsible actor remained unclear, which corresponds to the percentage in September. In 28 of the 79 total cases tracked for October, non-state actors were publicly identified, which roughly represents a 4% increase from the previous month. Of these 28 cases, 16 were attributed to ideologically- or politically-motivated hacktivists, while 12 were attributed to financially-motivated cybercriminals, or were at least claimed by these actors.

Russia, North Korea, and Ukraine tied as countries of origin for the most cyber operations recorded in October, with 5 operations each. These developments overlap with a sharp increase in the number of incidents occurring in the context of Russia's war against Ukraine (10 incidents) compared to September (3). In line with the overarching trend of recent months, China and Iran also figured among the prevalent countries of origin in October.

With Kazakhstan and Jordan, two countries placed among key points of origin in October that had not previously registered at this level since the start of the tracking for this briefing in April. However, the recorded cases differ from malicious activity linked to other countries: For the case relating to Kazakhstan, the threat intelligence department of Cisco, Talos, publicised a cyber espionage operation by the APT YoroTrooper, which had been spearphishing critical infrastructure and state targets in the Commonwealth of Independent States (CIS) since June 2023.



Suspected countries of origin of initiators October 2023

Number of operations per suspected initiating country

While industry reporting did not immediately connect the activity to government agencies, YoroTrooper attempted to draw suspicion to Azerbaijan as the country of origin of the espionage campaign as part of a false flag operation. In contrast, the hack-and-leak operation by Jordanian hacktivists against the Israeli Ono Academic College detected on 9 October, two days after Hamas' assault on Israel, fits extant patterns of hacktivist operations in the context of a violent conflict that quickly develops a transnational component, especially in cyberspace. This observation also parallels the hacktivist incidents observed in the context of Russia's war against Ukraine, where existing hacktivist formations quickly aligned themselves with the parties of the conflict in the wake of the invasion on 24 February 2022. For the conflict between Israel and Hamas, eleven incidents were recorded in the EuRepoC database in October 2023, exceeding the incident count for the Russia-Ukraine War by one. As the Repository only accounts for cases that have resulted in an observable information effect (i.e., a violation of confidentiality, integrity or availability) and which have been confirmed by independent third-party sources (in addition to any self-reported claims of the perpetrators), this number is significantly lower than in many media reports on the cyber component of the conflicts in the Middle East, some of which adopt the claims of attackers without verification. One example of such an unbacked, misleading claim was the alleged hack of the private Dorad power plant in Ashkelon on 8 October, just one day after the Hamas escalation. The pro-Iranian group Cyber Av3ngers had claimed an extensive DDoS attack on the critical infrastructure operator via social media and also presented purported evidence of this in the form of screenshots. However, these quickly turned out to be photos of a previous hack by the pro-Iranian group Moses Staff against an Israeli target from 2022. As illustrated in this case, accounts of politically-motivated hacktivism may be misleading about the form or extent of the achieved effects, even where the activity as such has been verified; in some cases, the operations may have been the work of a completely different group.

Accounting for such divergences in reporting, the level of cyber activity tracked by EuRepoC in the context of the Israel-Hamas conflict nonetheless has increased significantly since 7 October. Eight of the eleven incidents attributed to the conflict involved Israeli targets, two involved (pro-)Palestinian targets, and one involved a third party: Brazil. These developments also trace the activity patterns noted for Russia's war against Ukraine: The majority of activity is directed against the country under assault, with an additional proportion directed against targets on the side of the aggressor and against states/actors supporting the attacker. In this vein, Brazil may not appear as a likely target country for anti-Israeli/pro-Palestinian hackers. Although Brazil had submitted a draft resolution to the UN on 18 October condemning the violence of Hamas, the Brazilian government simultaneously continues to exert pressure on Israel to secure the release of hostages held by Hamas, including Brazilian hostages, even going so far as to call for a ceasefire. The incident could therefore also simply be an expression of the opportunistic target selection of some hacktivist groups, in which the technical vulnerability of a victim contributes to the targeting decision.

In a protracted military confrontation between Hamas and Israel, cyber operations against Israel and states that support it may continue to increase. The intensity and severity of these cases will also depend on the extent to which Iranian APTs side with Hamas. Analysts from Microsoft reported at a cyber security conference in early November that the behaviour of Iranian APTs exhibited no signs of prior knowledge of the attack by Hamas. However, some groups adapted their ongoing operations to support Hamas in the aftermath of October 7. According to Microsoft, this shift occurred only from 18 October onwards.

Recognising that Russia operates at a level several orders of magnitude higher than Hamas', both in terms of cyber and conventional capabilities, and - in contrast to Hamas - campaigns without significant dependence on a "cyber patron," the cyber conflict dynamics in the context of the Israel-Hamas conflict illustrate that conventional military firepower remains the decisive means of armed conflict resolution, in keeping with findings for the war against Ukraine. Cyber operations may play an ancillary role, potentially with a focus on generating psychological effects in target populations. As in the context of the war against Ukraine, examples of pro-Hamas hacks, e.g., against Israeli billboards, show that cyber operations in violent conflicts may aim at influencing the opposing population in the attempt to undermine public support or fighting morale. DDoS operations by the alleged Russian false flag group Anonymous Sudan against Israeli targets on 7 October could indicate that the hacktivist spheres of the two most violent geopolitical conflicts at present could share touching points in this psychological dimension, which could further complicate assessments of motivations and responsibilities.

Another conflict dyad in the Middle East with potential for impact on the course of the war between Hamas and Israel is the relationship between Iran and Saudi Arabia. While the two sides agreed to resume diplomatic relations in March 2023 under the mediation of the People's Republic of China (notably without the direct participation of the USA), Iranian cyber-enabled espionage against Saudi targets in August 2023, which only came to light in October, indicates that strategic cyber activity is likely to continue against the backdrop of high-level efforts at détente.

Considering that politically-motivated espionage is generally not regarded as illegal under international law, activities of this kind are rarely expected to lead to escalations within a conflict dyad, insofar as they are not suspected to directly prepare disruptive operations or to enable disinformation components as part of hack-and-leak operation. In situations of persisting mutual mistrust, cyber espionage operations may be considered a legitimate tool by states to ascertain whether political counterparts are (not) complying with the obligations laid down in intergovernmental agreements.

More from EuRepoC

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