European
Repository of
Cyber Incidents

EuRepoC Cyber Conflict Briefing

2023 CYBER ACTIVITY BALANCE

Jakob Bund
Kerstin Zettl-Schabath
Martin Müller
Camille Borrett

TABLE OF CONTENTS

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. In this special edition, we review all incidents recorded in 2023. These do not necessarily have to have taken place in 2023, 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

1 Overall observations

1.1. Number of new cyber operations recorded

895

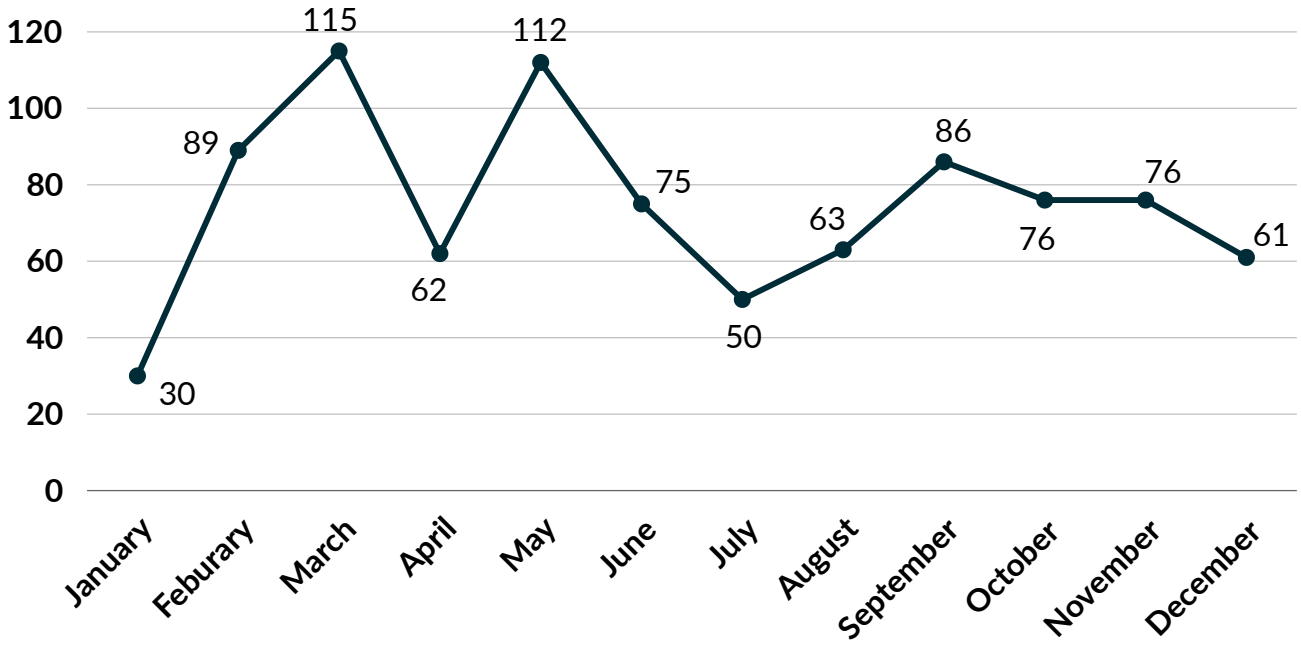
New cyber operations recorded in 2023

75

Operations on average per month

In 2023, the European Repository of Cyber Incidents (EuRepoC) recorded a total of **895 new cyber operations**, averaging about 75 operations per month. There were notable spikes in reported activity during March and May, with 115 and 112 new operations recorded in these months, respectively. In contrast, the summer months saw a decline in reported operations.

Number of cyber operations recorded per month in 2023:

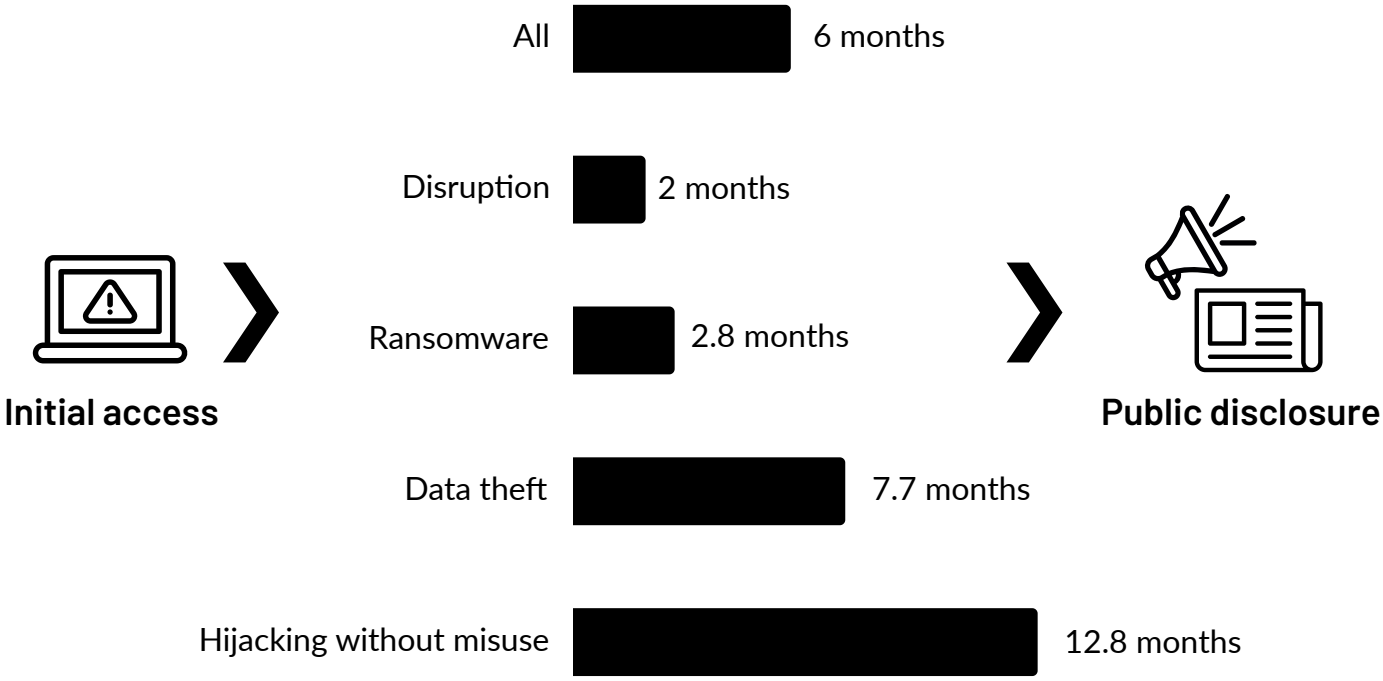


1.2. Time between initial access and public disclosure

The Repository records data on cyber operations from various sources, including IT community blogs, government reports, and media articles as they are reported. The recorded month of an operation does not necessarily align with its actual start date.

On average, the cyber operations recorded in 2023 started **approximately six months prior to when they were publicly disclosed**. The speed of disclosure varied by the nature of the cyber operation. Operations involving disruption and/or ransomware were generally revealed quicker, typically within 2 to 2.8 months, likely on account of their more visible effects and incentives for threat actors to claim credit for activities and exaggerate their impact. Whereas operations characterised by data theft and/or hijacking without misuse were often reported much later, averaging 7.7 and 12.8 months after initial access, respectively.

Number of months between initial access and public disclosure of cyber operation recorded in 2023:

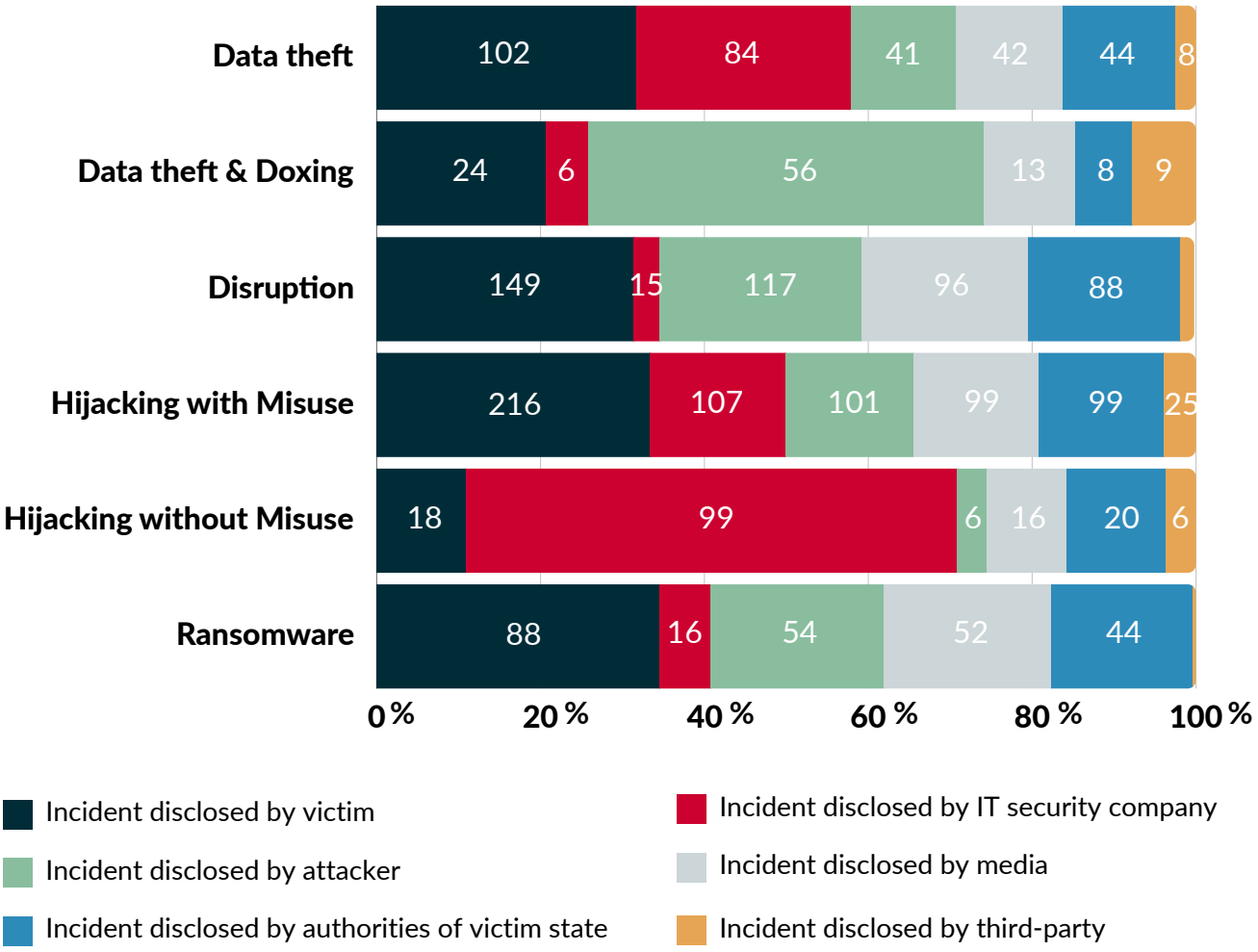


1.3. Who discloses cyber operations?

The largest share of cyber operations recorded in 2023, were disclosed by the **victim of the incident** (29%, 264 in total), followed by **IT security companies** (24%, 212 in total). In 21% of cases (189 in total) the operation was advertised by the threat actor, while 17% (148 in total) were reported by government authorities of the victim state.

Differences, again, can be observed by type of operation. The majority of operations involving hijacking without misuse (60%) were disclosed by IT security companies, while most data theft and leak operations (48%), very visible by nature, were disclosed by the responsible threat actors directly.

Source of disclosure of cyber operations by operation type in 2023:



Note: Individual cyber incidents may have several disclosure sources in combination

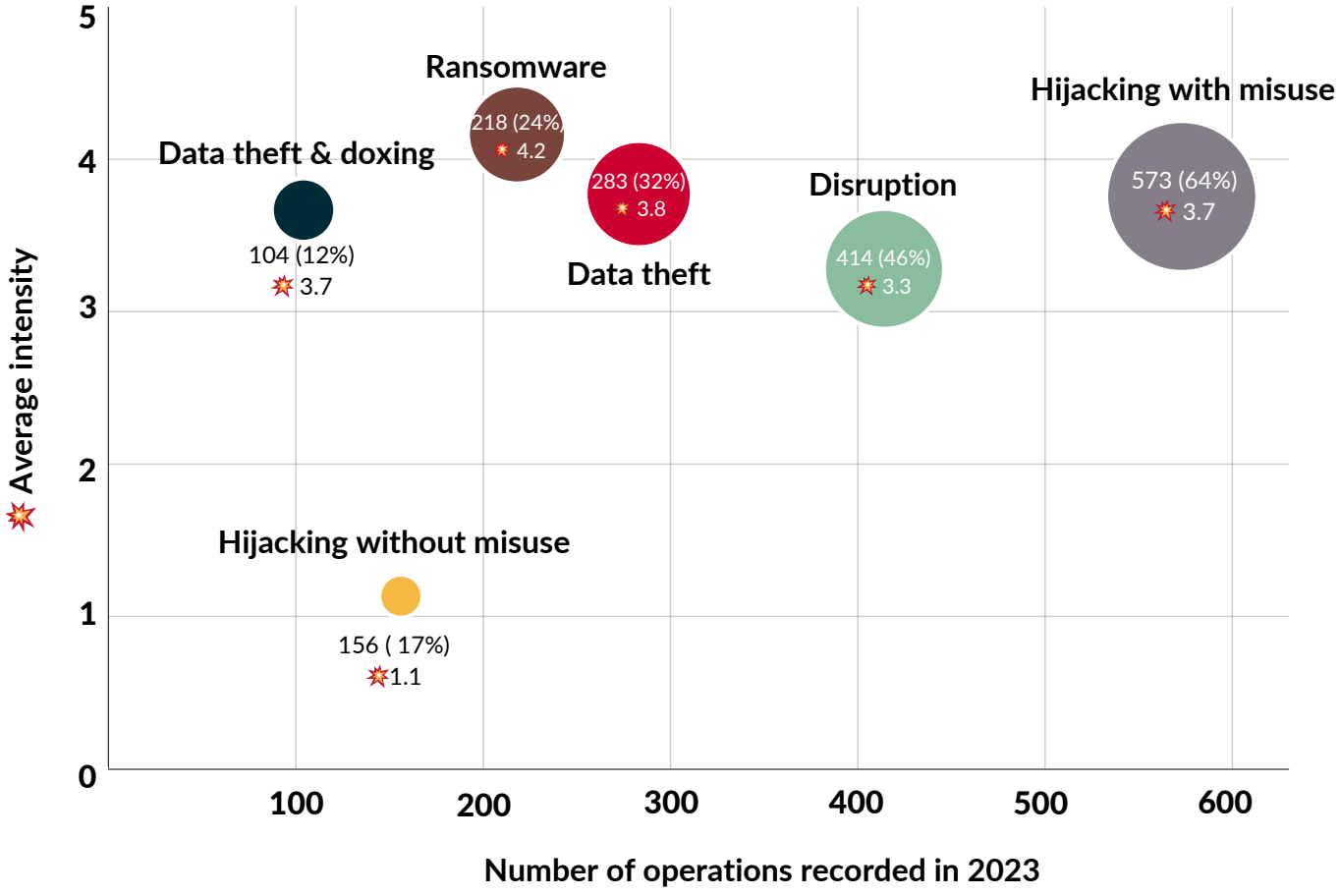
2 Distribution of operations

2.1. Types of operations and their intensity

In 2023, the most frequently recorded type of cyber operation was **hijacking with misuse**, totaling 573 operations (64% of all operations). Nearly half (47%) of these hijacking with misuse operations were combined with data theft (269 in total). The second most prevalent type was **disruption**, with a total of 414 operations (46% of all operations).

However, in terms of intensity, **ransomware operations stood out with the highest average intensity level (4.2)**. In comparison, less technically sophisticated disruption operations, such as DDoS attacks and defacements, and hijacking attempts to establish access without further misuse were less intense, averaging 3.3 and 1.1, respectively.

Distribution of cyber operations recorded in 2023 by intensity:



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

Cyber operations of notable intensity recorded in 2023:

Sandworm targets Ukraine's energy sector in apparent synchronisation with missile attacks

 **Russian Sandworm group** →  **Ukrainian critical infrastructure**

 **Intensity score: 9**

 **Disruption; Hijacking with misuse**

Sandworm, a threat actor with a track record of critical infrastructure attacks, infiltrated a Ukrainian energy organisation and caused a power outage amid Russian missile strikes against Ukrainian utilities in October 2022. Sandworm subsequently deployed an updated version of the CADDYWIPER against the victim's IT environment, to amplify disruptions and possibly impede investigations of the incident. The group's previous targeting of civilian infrastructure has been the subject of formal requests to the Office of the Prosecutor for the International Criminal Court to open an investigation into potential war crimes. Reaching an intensity score of 9, the operation from October 2022 exceeds the average intensity of Russian state-linked groups against Ukraine even during times of war. Considering the fact that Sandworm already had the opportunity to conduct the operation prior to this rocket 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 discovery of attack paths and 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.

2.2. Use of zero-days

22 cyber operations recorded in 2023 made use of a zero day, two of which involved multiple zero days, of which 9 were for operations that took place in 2023. This is on par with 2022, in which 10 cyber operations initiated in the year made use of zero days. It took on average 15 months to publicly attribute incidents with zero days reported in 2023, this is 5 additional months on average compared to incidents without zero days.

By comparison, Project Zero, an initiative of Google security researchers tracking the use of unreported vulnerabilities, documented the exploitation of 55 zero days in the wild for 2023. This marks an increase of 34% over 2022 but is down by 20% from the all-time high of 69 zero days Google registered for 2021.

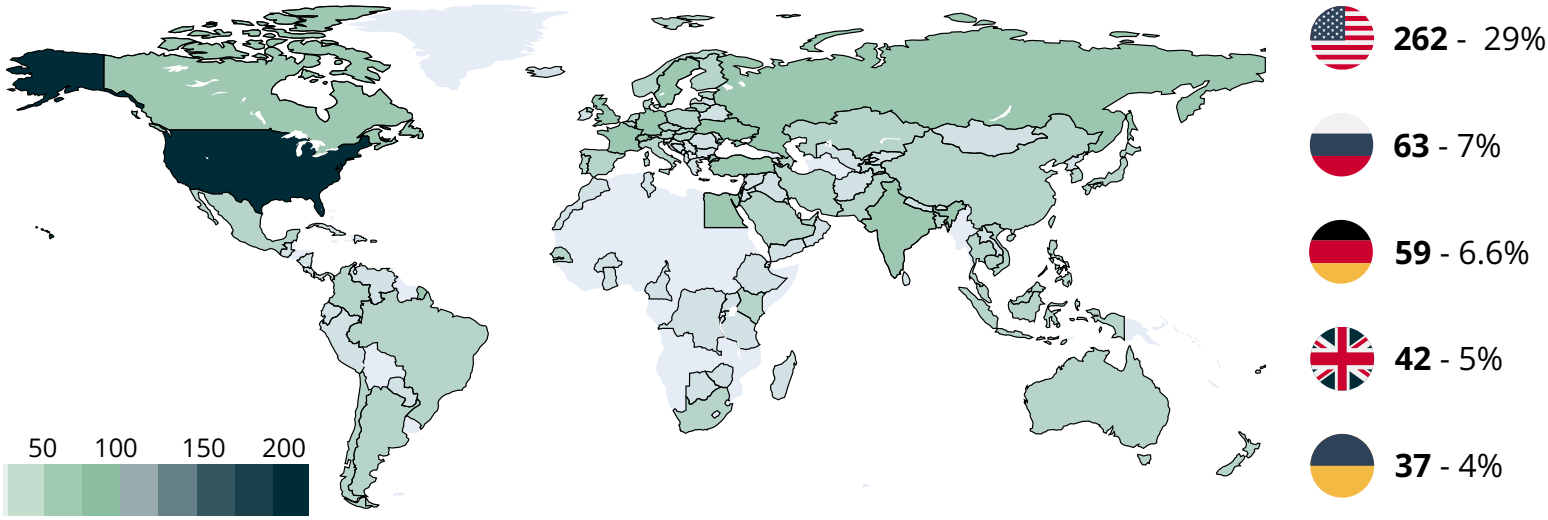
The overlap in zero day usage between EuRepoC and Project Zero data reflects the large share of previously unknown vulnerabilities in operations conducted by well-resourced state-backed actors as well as operations against hardened critical infrastructure targets - types of threat activity that are in the focus of the incident tracking undertaken by EuRepoC.

3 Targeted countries and sectors

3.1 Geographical distribution of operations

In 2023, cyber operations predominantly targeted the **United States**, which faced 262 incidents and was targeted 4 times more than **Russia**, the next most targeted country, with 63 incidents. The US and Russia were followed by **Germany** with 59 incidents, the **United Kingdom** with 42 and **Ukraine** with 37 incidents.

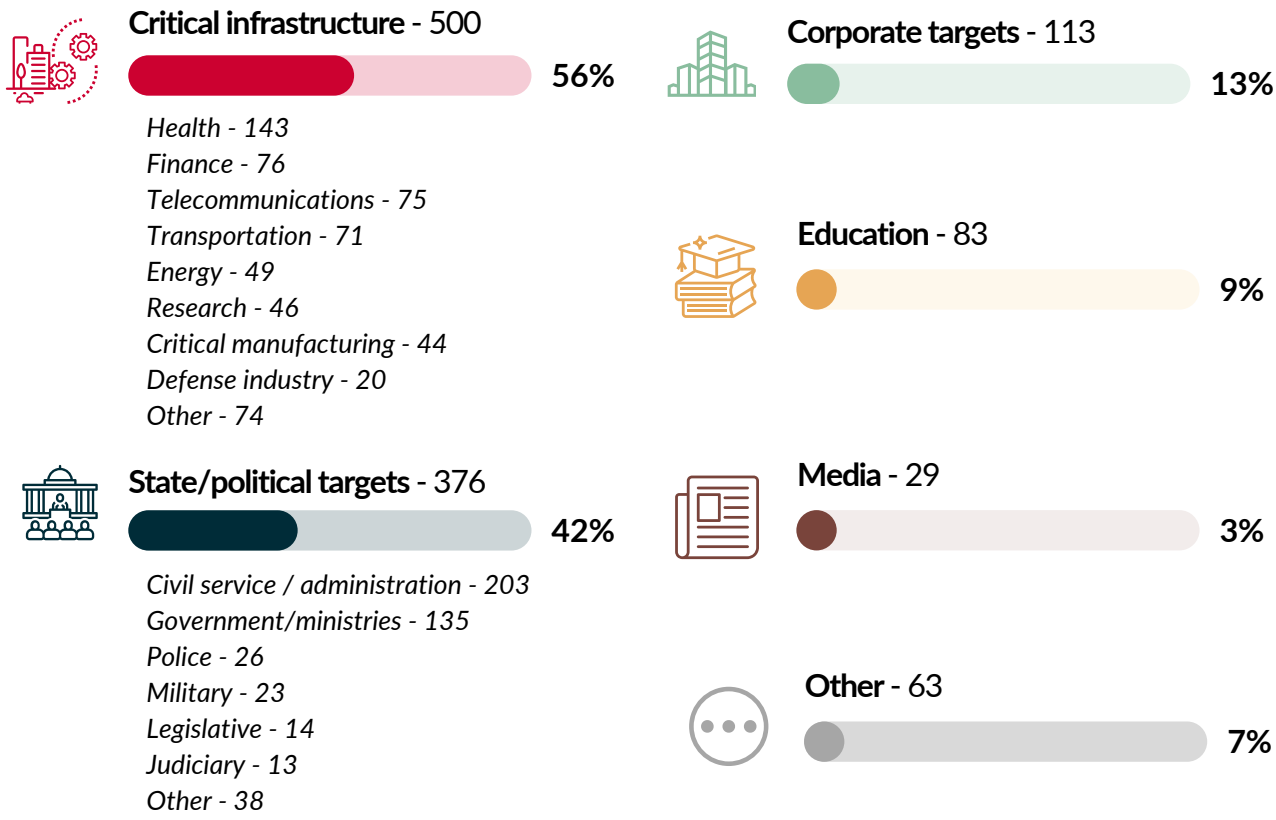
Number of cyber operations by targeted country recorded in 2023:



3.2 Targeted sectors

More than half of the cyber operations recorded in 2023 (56%) targeted critical infrastructure, notably the health, finance, and telecommunications sectors. The health sector in particular accounted for 16% of all new cyber operations, totaling 143 incidents. **State institutions and political systems** were the second most frequently targeted sector, representing 42% of new recorded operations. The main subcategories were civil service and administration, which faced 203 incidents, and government/ministries with 135 incidents.

Number of cyber operations by targeted sector in 2023:



Note: Individual cyber incidents may target multiple sectors and sub-sectors.

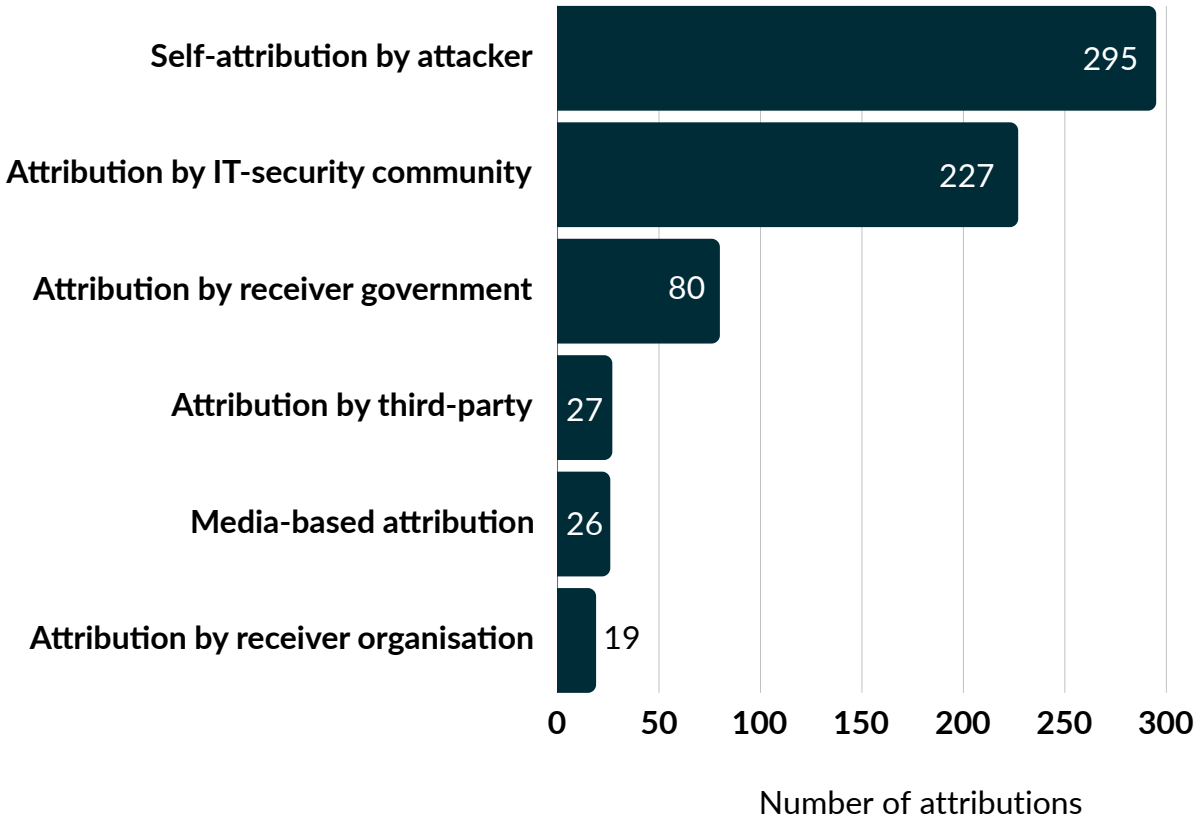
4 Attributions and threat actor profiles

4.1 Attribution bases

Almost two-thirds (65%) of the cyber operations recorded in 2023 had at least one public attribution reference assigned. While most operations had a single attribution anchor, some had up to six different attribution assessments, amounting to a **total of 650 attribution findings recorded across all incidents**. In most cases, threat actors directly claimed responsibility n the course of or following an operation (45% of attributions).

Self-attributions by ransomware-gangs or hacktivists are still the most common source of public attributions. The IT security community was the second most common source of attribution, representing 35% of attributions for incidents tracked by EuRepoC in 2023.

Attribution bases in 2023: who attributed the most in 2023?

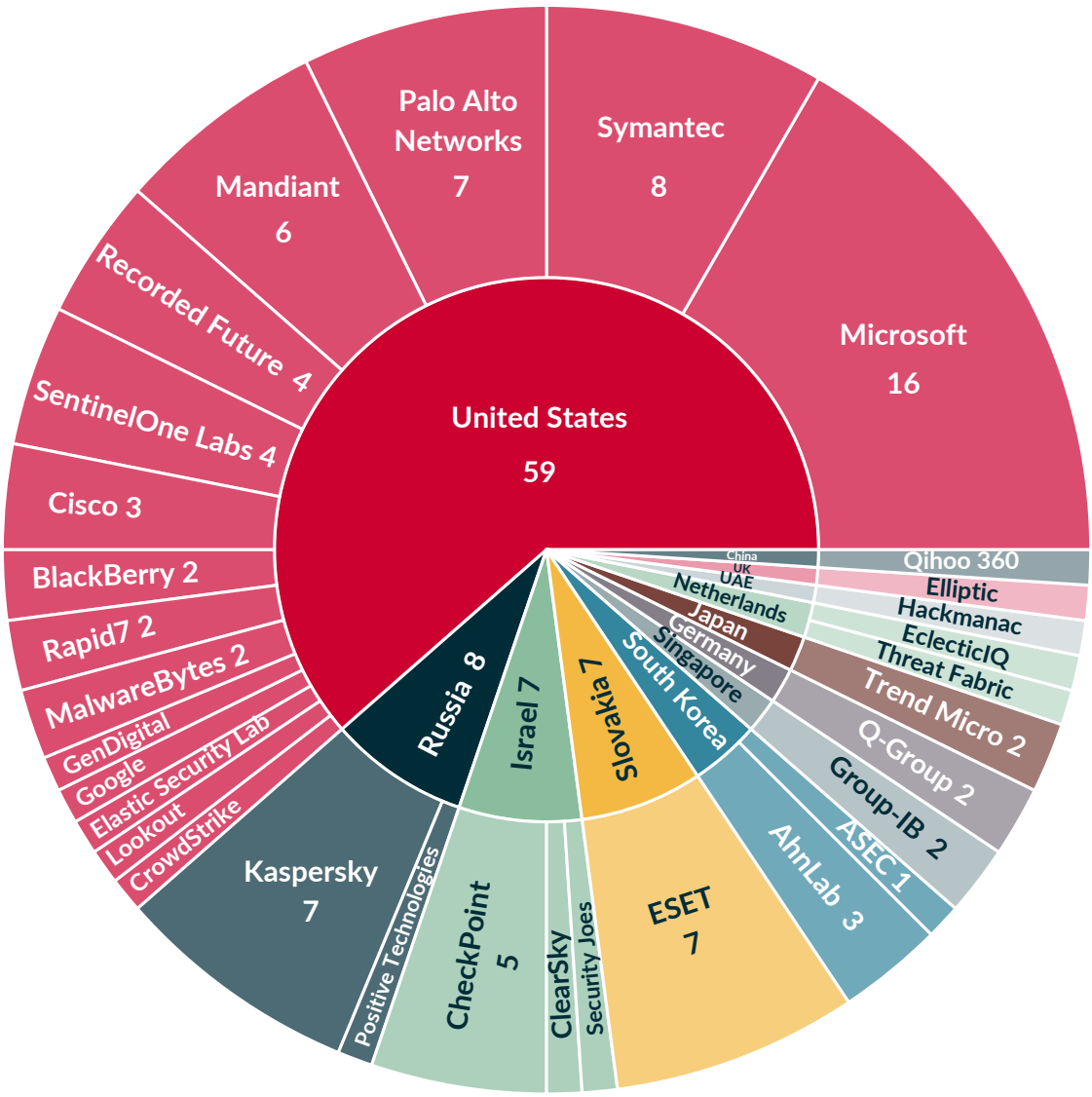


4.2 Attribution by IT/Threat intelligence companies

Among IT entities, the leading attributors tracked by the Repository were **Microsoft** with 16 attributed operations, **Symantec** with 8, **ESET**, **Kaspersky**, and **Palo Alto Networks**, each with 7 attributed operations and **Mandiant** with 6.

Threat intelligence companies incorporated in the **United States** continue to lead attribution statistics, followed by **Russian** companies, with Kaspersky as the dominant player following Group-IB's withdrawal from Russia in early 2023, and enterprises from the "start-up nation" **Israel**.

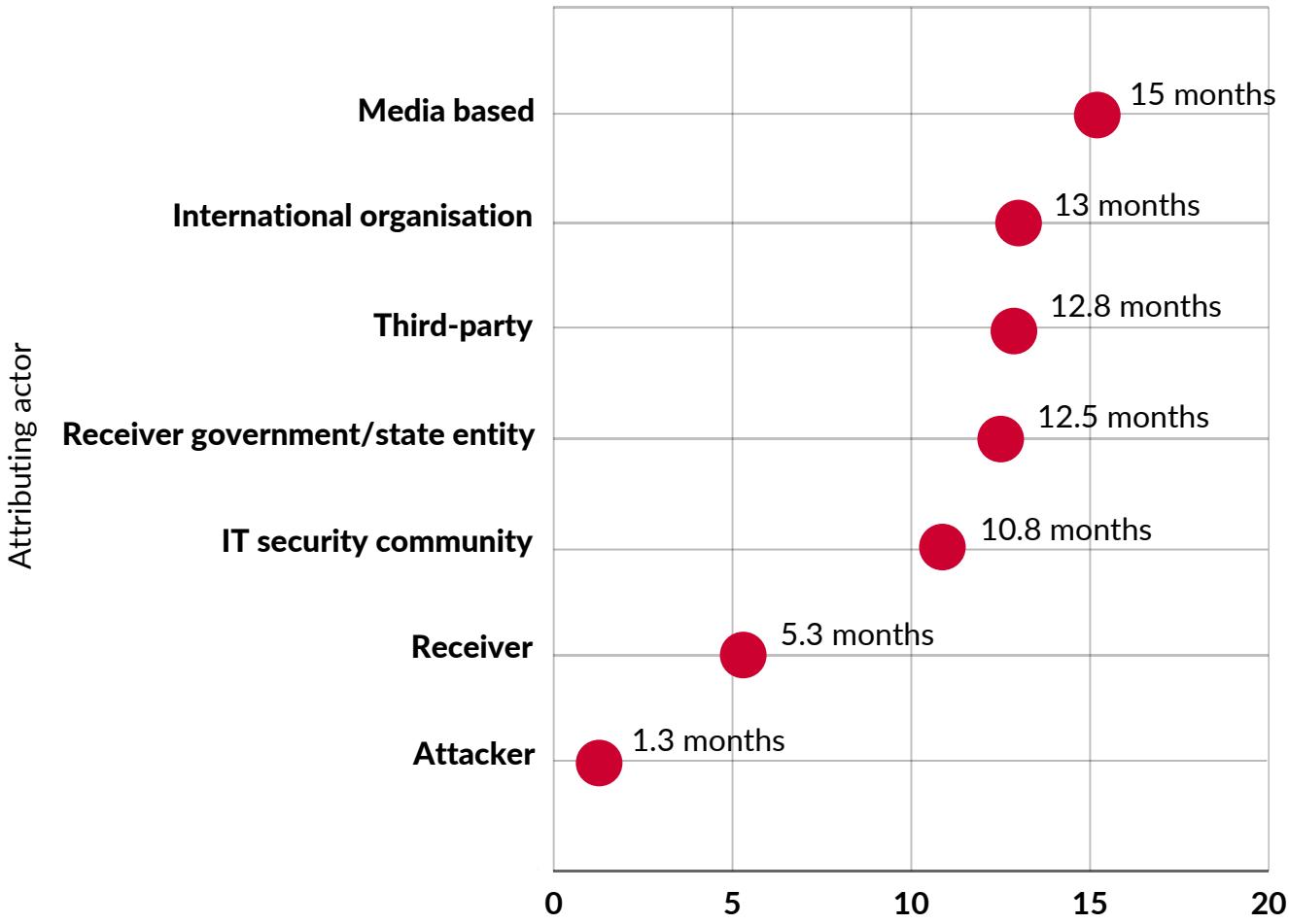
Number of cyber operations attributed by IT/Threat intelligence companies in 2023:



4.3 Speed of attribution

In 2023, for all recorded cyber operations, public attributions were made, on average, **10 months after the operation's recorded start date**. The timeframe for these attributions varied significantly, depending on the source of the attribution. When attackers self-attributed their operations, attributions came as quickly as within 1 month. In contrast, attributions from media sources took as long as 15 months. Furthermore, government entities took an average of 2 months longer than IT community companies to attribute cyber operations in which they were the targets. Thus, although governments still need more time to publicly attribute, the average time between technical and political attribution is expected to continue to decrease in the future.

Average time between recorded incident start date and its attribution:



Average number of months between recorded incident start date and its attribution

4.4 Contested and new attributions

Only **five incidents added in 2023 included contested attributions/information**: In one case, the Akira ransomware gang denied its involvement, instead declaring its ransomware suite had been hijacked by another threat actor. Another incident was assessed as an alleged Ukrainian false-flag operation masquerading as the Russian Wagner group. Moreover, the collective operating under the moniker Anonymous Sudan have claimed responsibility for multiple incidents. The credibility of the group's links to Sudan have been called into question by several threat intelligence companies, suspecting a connection to the Russian hacktivist group Killnet. Finally, two ransomware gangs claimed responsibility for the same hack against Sony.

Attribution is often work-in-progress, involving multiple attribution steps, adding new information to the characterisation of the suspected threat actor over time. The Repository recorded **five new attribution statements** published in 2023 for **previously covered incidents**. One of them concerned two operations that had already taken place in 2015 and 2016 and which were published the following year. Thus, attribution, like cybersecurity, should be perceived as a process rather than a final status.

4.5 Political attributions

With **12%, attributions from governments/state entities of targeted countries** made up a comparatively small share. The **United States** topped the list with 28 attributions, followed by **Ukraine** (13), the **United Kingdom** (7), and **South Korea** (6). This also corresponds with the high numbers of recorded cyber incidents against the US and Ukraine in particular in 2023.

Germany attributed only 2 out of the 59 incidents recorded in 2023 that targeted entities within the country. The Federal Office for the Protection of the Constitution attributed North Korean state-sponsored hacking group Kimsuky for an incident against German research institutes in March 2023. The German Ministry of Interior attributed the Akira ransomware group which targeted the IT service provider Südwestfalen-IT on 29 October 2023. The attribution rate for German government actors thus stood at 3%. This ratio is lower than those of the UK and US counterparts, which clock attribution rates of 17% and 11%, respectively.

4.6 Joint political attributions

Several recorded incidents included 'joint attributions' by affected government entities of multiple countries. These attribution networks may indicate patterns of 'like-mindedness' in publicly condemning and attributing cyber-attacks. At the same time, joint attributions require a certain degree of information sharing, reflecting a significant amount of trust between the attribution partners. Notably, the US not only increasingly publishes joint attribution statements by various domestic authorities/agencies, but also regularly partners with allies for joint cross-border attributions. Those partner countries, such as Japan, South Korea or Ukraine, reflect regional hotspots of wider geostrategic importance in both the conventional and cyber sphere.

Cyber operations with joint attributions by receiver governments in 2023:

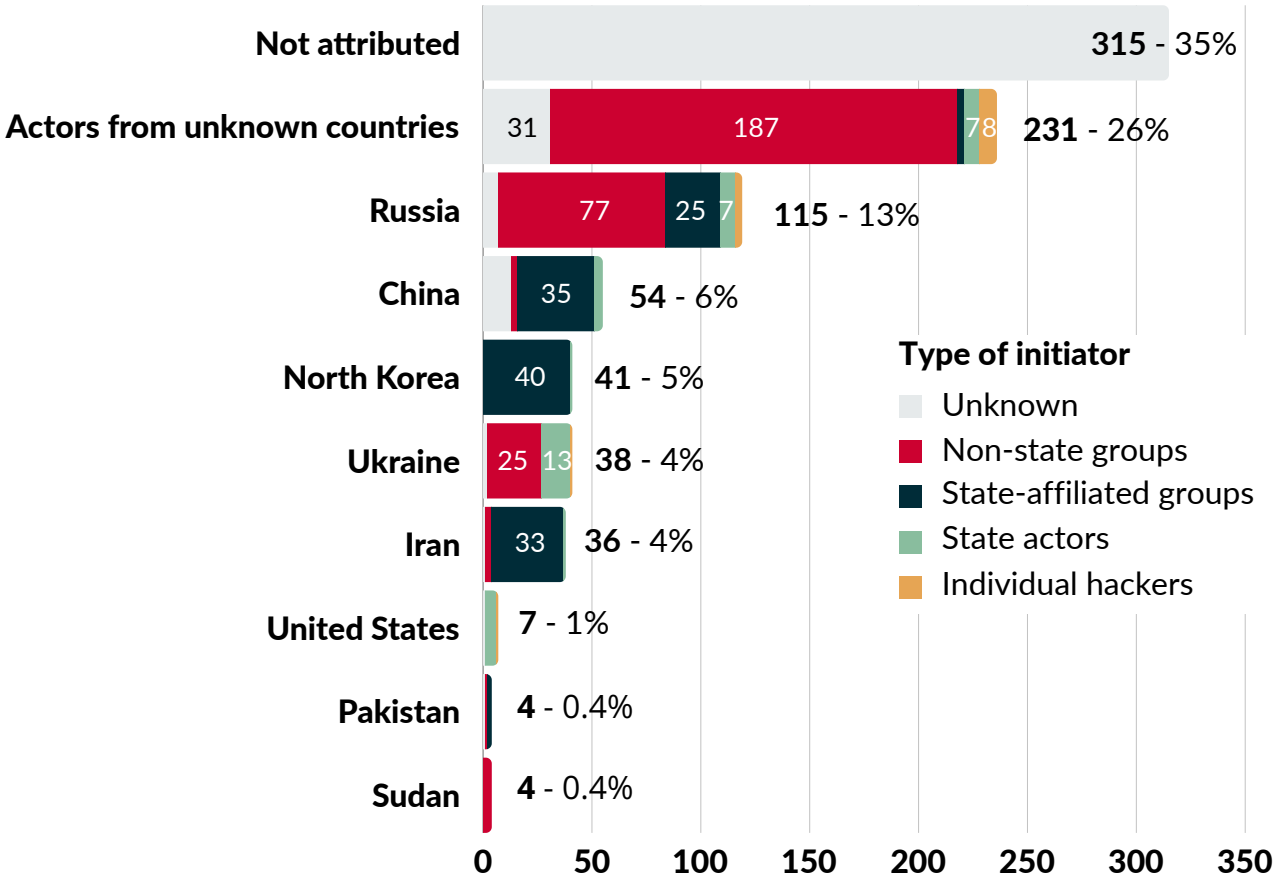
	2	-North Korean sponsored Andariel stole sensitive information from South Korean defense and pharmaceuticals companies and research institutes -Andariel disrupted US and South Korean healthcare providers and other critical infrastructure with ransomware attacks
	1	Chinese threat actor 'BlackTech' targeted international subsidiaries of US and Japanese companies
	1	Russian sponsored APT28 accessed Roundcube servers of various Ukrainian targets
	1	Russian sponsored APT28 accessed unpatched Cisco routers from European, U.S. and Ukrainian targets
	1	Russian sponsored APT29 accessed servers hosting JetBrains TeamCity software
Five Eyes	1	Chinese sponsored Volt Typhoon accessed a variety of critical infrastructure organizations on Guam and the US mainland
	1	North Korean sponsored Kimsuky stole emails from South Korean and German research institutes
	1	North Korean Lazarus group attack against South Korean software maker

4.7 Suspected origin of cyber operations

Remaining blind spots: For 35% of the operations recorded in 2023 the initiator remains unattributed. For a smaller set, 26%, the country of origin is unknown. A significant number of operations (187 or 21%) were initiated by **non-state groups of unidentified origin.**

Russian and **Chinese threat groups** recorded the most activity in 2023, with 13% and 6% of operations documented as initiated by actors in these two countries. In Russia, these were predominantly non-state groups (notably NoName057(16) and Killnet), whereas in China, a significant portion were state-affiliated groups (65% of incidents initiated from China), with Mustang Panda and UNC 2814/Gallium engaging as prolific actors.

Number of cyber operations by suspected country of origin in 2023:



4.8 Operations by state or state-affiliated actors

States can pursue different short or long-term goals through their (or their proxies') cyber operations. For Russia, the distribution of incident types recorded in the EuRepoC database reflects the dominance of operations in the context of the war against Ukraine, including cyber espionage and more disruptive operations, such as wiper attacks, that are coded as a combination of "hijacking with misuse" and "disruption" in the Repository. By contrast, Ukrainian cyber operations focused more on data theft and doxing, reflective of an approach to secure supportive international public opinion and potentially influence Russian domestic views on the war, borrowing from hack-and-leak tactics Russia has deployed outside of already escalated conflicts.

In comparison, Chinese cyber operations more often involved a recorded infiltration of target systems, without further reported impact, coded as "hijacking without misuse". In line with previous reporting by threat intelligence companies, this mirrors the Chinese approach of establishing beachheads in strategically important adversary networks in order to conduct potential sabotage operations against them in case of conflict escalations in the future. The comparatively high number of such cases for Iranian actors also suggests a potentially similar tactic for the regime in Tehran. Four of the five recorded operations attributed to state/state-affiliated actors from the US were conducted by the FBI, as part of its expanding disruption campaigns against criminal and state-sponsored hacking networks.

Number of cyber operations initiated by state and state-affiliated groups by top country of origin in 2023:

	Hijacking with misuse	Hijacking without misuse	Disruption	Data theft	Data theft & doxing	Ransom-ware	Total incidents *(may have multiple types)*
Russia	25	6	10	14	2	0	**32**
China	14	22	0	17	0	0	**38**
North Korea	18	23	2	10	0	2	**41**
Ukraine	13	0	5	2	9	0	**13**
Iran	15	19	7	8	3	2	**34**
USA	5	0	3	3	1	0	**5**

4.9 Threat actor profiles

2023 was marked by a prevalence of hacktivist operations related to Russia's war against Ukraine, but also a multitude of ransomware cases, as recorded by EuRepoC. Accordingly, NoName057(16) and two prominent ransomware gangs are among the initiator groups, for which the Repository added the most incidents in 2023. In contrast, the high activity rate of the North-Korean Lazarus group as a state-controlled APT reflects the continuing appeal of cyber operations for the North Korean regime, as a tool to obtain military technology and generate financial resources via hacks of banks or crypto entities. Continuing a pattern observed for hacktivists and ransomware operations, self-attribution played an important role for the reported cyber operations by the Ukrainian defence intelligence service. Where threat actors stand to gain from making their operations public or the effectiveness of an operation is linked to publicity, the absolute number of operations attributed to the initiator is expected to be higher than for actors whose operations thrive on secrecy.

Most prolific initiators in 2023 *(by number of operations)*

Name	Origin	Type	Ops in 2023	Main type of operation	Main targeted sectors
NoName057(16)		Hacktivist group	31	Disruption	• Gov/ministries • Transport • Finance
Lazarus Group		State-affiliated	30	Hijacking	• Finance • Corporate targets • Defense industry
LockBit		Ransomware group	21	Ransomware	• Transportation • Civil service/admin
Medusa		Ransomware group	13	Ransomware	• Civil service/admin • Education • Research
GURMO		State group	13	Hijacking	• Energy • Corporate targets

LockBit, identified as the most active global ransomware group by the Five Eyes states together with France and Germany, is the only threat actor ranking both among the most prolific initiators and the actors for whom the Repository has tracked the highest average intensity per operation in 2023.

Ransomware gangs more broadly dominate the intensity ranking, which can mainly be explained by the way EuRepoC assesses intensity: calculations of the intensity score are based on the individual intensity rating of each incident type identified for one operation. Since ransomware operations regularly combine several incident types, including not only disruption and hijacking with misuse, but in case of double-extortion schemes also data theft (sometimes in combination with doxing), this often results in a higher intensity score, due to the higher number of coded incident types. At the same time, it also demonstrates the complexity and flexibility of ransomware as an extortion scheme. Reports already point to *triple extortion* schemes, where threat actors contact the target's customers or partners, informing them about their potential data disclosure if the targeted company/actor refuses to pay the victim, with the ultimate goal of increasing the pressure on the latter. *Quadruple extortion* expand on these tactics by threating to take down the victim's servers/networks with a DDoS attack in case the ransom payment is refused.

The notification of public authorities by ransomware gangs about the alleged violation of disclosure requirements by their victims could add another level of extortion.
Among APTs, the Russia nexus group Sandworm figures as the actor with the highest average intensity score. The group acts in accordance with the military goals of the Russian intelligence service GRU, especially against Ukrainian targets pursuing physical effects, which remain the exception.

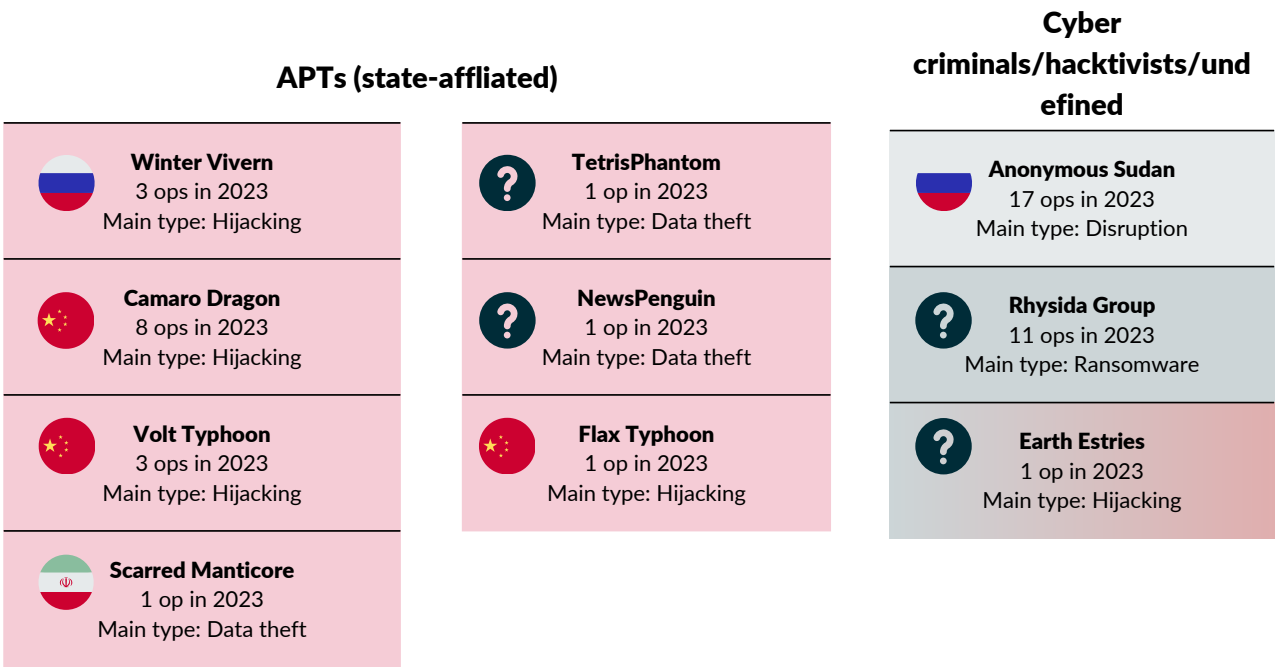
Most intense initiators in 2023 (by intensity of operations)

Name	Origin	Type	Intensity	Main type of operation	Main targeted sectors
LockBit		Ransomware group	5	Ransomware	• Transportation • Civil service/admin
Rhysida Group		Ransomware group	4.2	Ransomware	• Civil service/admin
PLAY		Ransomware group	4.2	Ransomware	• Transport • Corporate targets
Sandworm		State-affiliated	4	Hijacking	• Critical infrastructure
BlackCat		Ransomware group	4	Ransomware	• Critical infrastructure

4.10 EuRepoC “newcomers” in 2023

2023 also saw the emergence of **new attacker groups** not previously covered by the EuRepoC database. Three out of seven APTs recorded for the first time were attributed to China as state-sponsor, followed by a new Russian and Iranian group, also with a purported state-nexus. This observation reflects the thriving Chinese cyber-ecosystem, with an increased level of reported tool-sharing among state-affiliated groups on the one hand, but also an expansion of delegated tasks in cyberspace on the other, leading to the formation of new hacking groups.

As the ransomware ecosystem continues to expand and groups reorganise to eschew law enforcement investigations, EuRepoC began covering a previously untracked cyber-crime gang, conducting ransomware operations in 2023. However, as is often the case with ransomware gangs, assessments vary as to whether Rhysida constitutes a new group with different members, or whether the Vice Society group, which has been active since 2021, started using the Rhysida ransomware from May 2023.



5 Political and legal context

5.1 Main related offline conflicts

The Repository recorded a number of cyber operations directly linked to ongoing offline conflicts in 2023:

	**Russia-Ukraine war**	140
	**Iran-Israel conflict**	14 (7 from 7/10/2023)
	**Israeli-Palestinian conflict**	13 (12 from 7/10/2023)
	**North Korea-South Korea conflict**	8

The listed conflict dyads reflect an already established finding of cyber conflict research, namely that cyber operations are often used in the context of regional and therefore often already violently escalated conflicts (also called "enduring rivals"). In these contexts, cyber capabilities are usually deployed only in addition to conventional military means and not as a substitute.

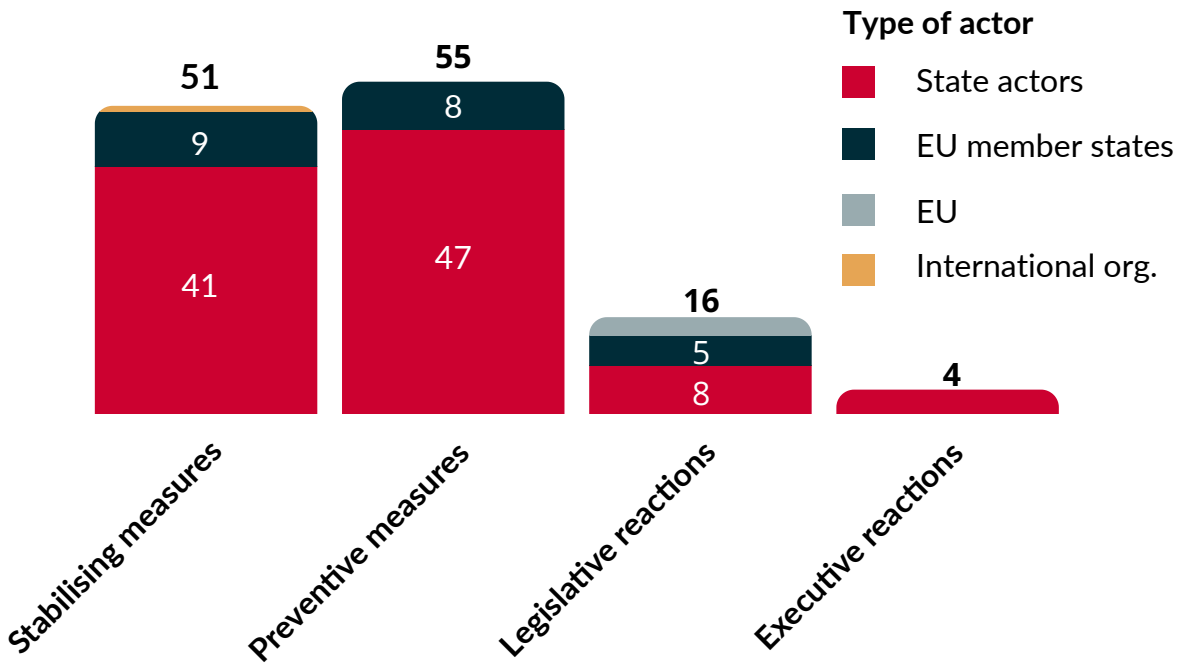
The Russia-Ukraine war was the source of 16% of the operations recorded in 2023. Of these, 37% (52 in total) targeted either Russia or Ukraine, with 35 incidents (25%) initiated by Ukrainian groups against Russian targets and 17 (13%) initiated by Russian groups against Ukrainian targets. In addition, a similar proportion of these operations (38% or 51 in total) were incidents initiated by groups of Russian origin (mainly non-state groups) against countries supporting Ukraine, particularly the US and EU member states.

The conflict between Iran and Israel is a distant second in terms of numbers, followed by the Israel-Hamas conflict. Activities linked to the latter were primarily recorded after the violent escalation on 7 October 2023. It is hard to assess whether and, if so, which Iranian-sponsored cyber incidents were conducted in support of Hamas, due to the long history of disruptive and espionage operations between Iran and Israel. Given the notable increase in recorded operations originating from Iran against Israeli targets since 7 October, a correlation at least seems plausible.

5.2 Political responses

In 2023, a **total of 108 cyber operations (12% of all recorded events) elicited political responses.** These responses were categorized as follows:

Types of political responses in 2023:



Note: Individual cyber incidents may have multiple political responses.

Stabilising measures refer to statements by government officials or officials of international and supranational organisations, while preventive measures comprise awareness raising efforts by cybersecurity agencies, such as CISA in the US, the Ukrainian CERT-UA or the German BSI. Preventive measures further include confidence- and capacity-building initiatives by states in third countries which might be underrepresented in the database as these undertakings are not consistently publicly reported or not explicitly framed as responses to specific cyber operations (for examples see here and here). Legislative measures largely concern statements by opposition parties in parliament or parliamentary investigation committees. The Repository's classification of these response measures is based on the EU Cyber Diplomacy Toolbox (CDT). While legally these measures refer to instruments of the EU and its member states, the CDT as an assessment framework offers a yardstick for taking stock of the measures adopted by third countries.

The **United States** led in issuing political responses for 35 operations. The majority of these were preventive measures (24), followed by stabilising measures (10). **Ukraine** responded politically to 10 incidents, through preventive measures by CERT-UA. **Germany**'s political response to 10 operations in total varied by type, including legislative measures (6) concerning mainly a DDoS attack in April 2023, preventive measures (4), and stabilising measures (3).

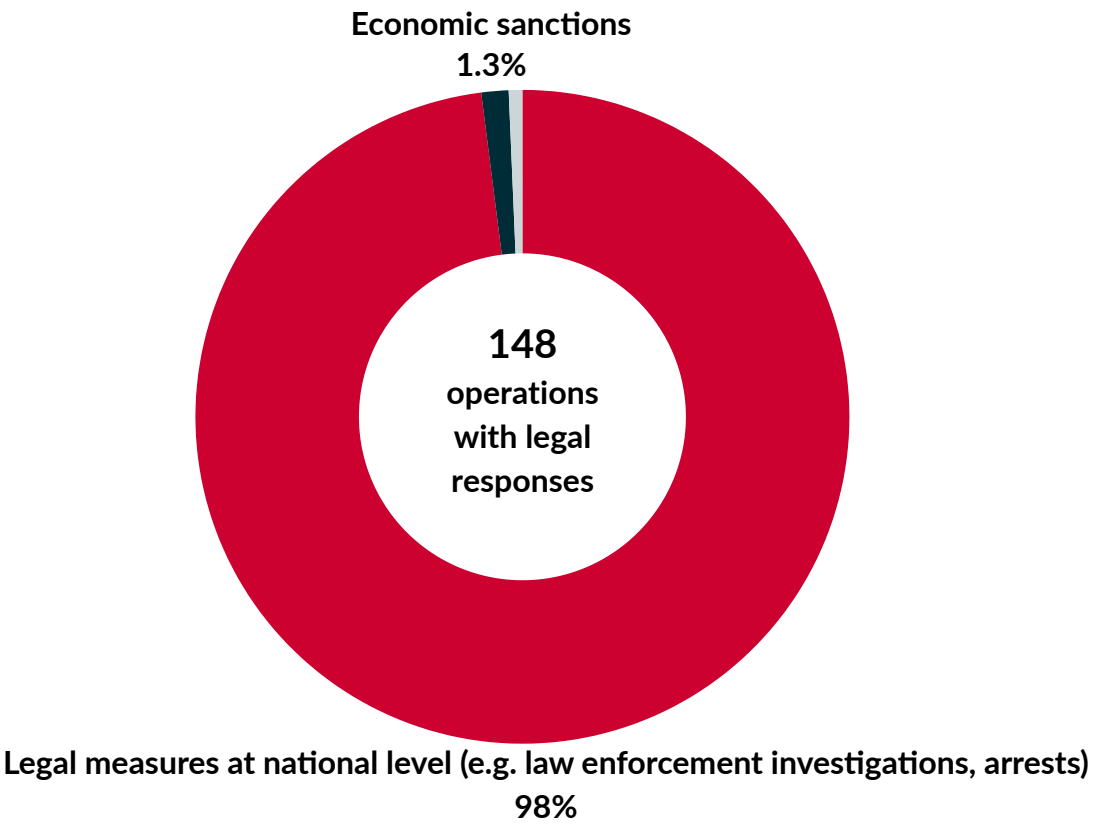
5.3 Legal responses

16.5% (148 in total) of cyber operations recorded in 2023 were met with a legal response. These responses were predominantly national-level measures (98%). Most of these measures were reports that law enforcement investigations were initiated. For only a few incidents, the Repository recorded responses in 2023 extending to arrests and following legal proceedings, showing the difficulty for nation states to prosecute effectively. However, law enforcement agencies have had some success with coordinated takedowns of cybercriminal's infrastructure as demonstrated in the cases of Qakbot and ALPHV/BlackCat.

Two incidents drew economic sanctions from the United States. These two incidents were initiated by the Russian state-sponsored Callisto group, who conducted a spear-phishing campaign against the US Department of Energy beginning in May 2022 and against several US defense institutions beginning April 2022. In both cases Callisto likely pursued espionage objectives. Moreover, the UK and the US imposed sanctions in December 2023 against the group for interference in democratic processes in the UK.

The leading countries in issuing legal responses were the United States (61), followed by Germany (11), France (9), and the United Kingdom (8).

Types of legal responses in 2023:



Cyber operation with notable responses recorded in 2023:

Ransomware group Play targeted the Swiss IT service provider Xplain AG

Play ransomware group → **Swiss IT provider**

Intensity score: 5

Ransomware

In April 2023, the ransomware group Play targeted the Swiss IT service provider Xplain AG. Data of the company was encrypted, stolen and then published in full, a common procedure for Play when no ransom is paid. The incident stands out as Xplain AG provides IT solutions for the majority of Swiss authorities and that information classified as top secret was disclosed as part of the leaks. A crisis team was set up in response to the incident at a political level, while investigations by the Swiss security authorities and the data protection commissioner are continuing at a legal level. The incident has a significant impact score of 14, which is intended to determine the severity of a cyber incident from a political and legal perspective based on the criteria of the EU's Cyber Diplomacy Toolbox. The incident highlights the dependence of state institutions and private companies on external service providers, which are lucrative targets for various threat actors in the context of supply chain compromises.

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