Working Paper

SWP Working Papers are online publications within the purview of the respective Research Division. Unlike SWP Research Papers and SWP Comments they are not reviewed by the Institute.

SWP

RESEARCH DIVISION EU / EUROPE | WP NR. 03, FEBRUARY 2025

Cyber Activity Balance 2024: The European Union in Focus

Jakob Bund, Annegret Bendiek, Jonas Hemmelskamp

UNIVERSITÄT HEIDELBERG ZUKUNFT SEIT 1386
SWP Stiftung Wissenschaft und Politik German Institute for International and Security Affairs
CPI CYBER POLICY INSTITUTE
universität innsbruck
European Repository of Cyber Incidents

The persistent nature of threats enabled by cyber and information space (CIR) capabilities has put the response strategies of governments in Europe and beyond to the test. The cumulative gains cyber campaigns seek to develop challenge traditional diplomatic tools that are designed to impose one-off consequences.

To further the understanding of how foreign and security policy instruments can contribute to countering these threats, the *European Repository of Cyber Incidents* (EuRepoC) has been tracking cyber operations of political implication and state responses over two and a half decades.

The Repository combines this depth in data with the continuous daily expansion of the dataset to enable short-term and long-term trend analysis. Focusing on the EU landscape, the key findings presented in this 2024 edition of the Cyber Activity Balance[1] draw on EuRepoC's open-source based contribution to empirically-driven cyber peace and conflict research.

Ransomware attacks are leading on intensity

Following a surge in threat activity documented for the EU in 2023, activity remained at an elevated level in 2024. Operations against EU targets increased by 16%. Considering the slight decrease in the volume of operations tracked globally (excluding EU member states) of 6.3%, this development points to a concentration of malicious activity against EU targets in 2024.

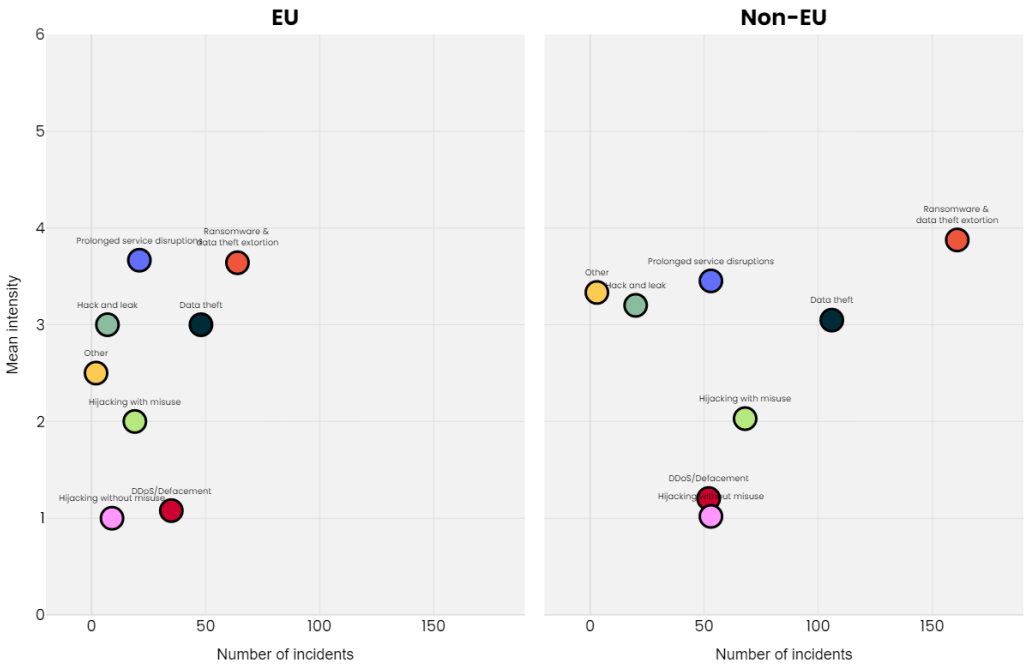
Among the operations tracked for 2024, ransomware and data extortion schemes show the highest intensity, both for targets within the EU and globally.

For critical infrastructure organizations and political organizations, the primary target space mapped by the Repository, ransomware-related threats retained a level similar to 2023, showing a slight increase in volume and a marginal drop in intensity.

This continuity in intensity reflects the disruption ransomware continues to cause, even as by some metrics the number and amount of ransom payments decreased in 2024. The blockchain analysis firm Chainalysis linked such findings to law enforcement successes in 2024 that disrupted criminal networks, returned ransom payments, and provided decryption keys to victims. This marks an impactful breakthrough considering the sustained high volume of ransomware attacks. Based on an attempt at a global accounting by the cybersecurity consulting company NCC Group, the 5236 attacks registered for 2024 constituted the largest number since the firm started its monitoring in 2021. Despite the internationally coordinated takedown of LockBit infrastructure in early 2024, the NCC statistics show the group as responsible for more incidents than any other actor, amounting to 10% of the tracked activity.

Whether these changes in victim behavior will influence the targeting pattern of ransomware groups remains a key point of analysis, in light of proposals to ban or require the reporting of ransom payments, including such consultations as announced by the UK National Cyber Security Centre in January 2025.

[1] The Cyber Activity Balance is part of the Cyber Conflict Briefing series, an analytic product prepared by EuRepoC. The English edition of the Cyber Activity Balance 2024 is published in parallel as EuRepoC report. A German version is published in collaboration with **Tagesspiegel Background - Cybersecurity.**



Volume and intensity of incidents by operation type, 2024

Criminal data theft is the most frequent threat for telecommunication companies in the EU

Ransomware and data theft extortion remains a cross-sector threat, indicative of the opportunistic targeting practices by criminal syndicates that seek to exploit vulnerabilities where they find them.

Among critical infrastructure organizations in the EU, the health sector was most frequently targeted.

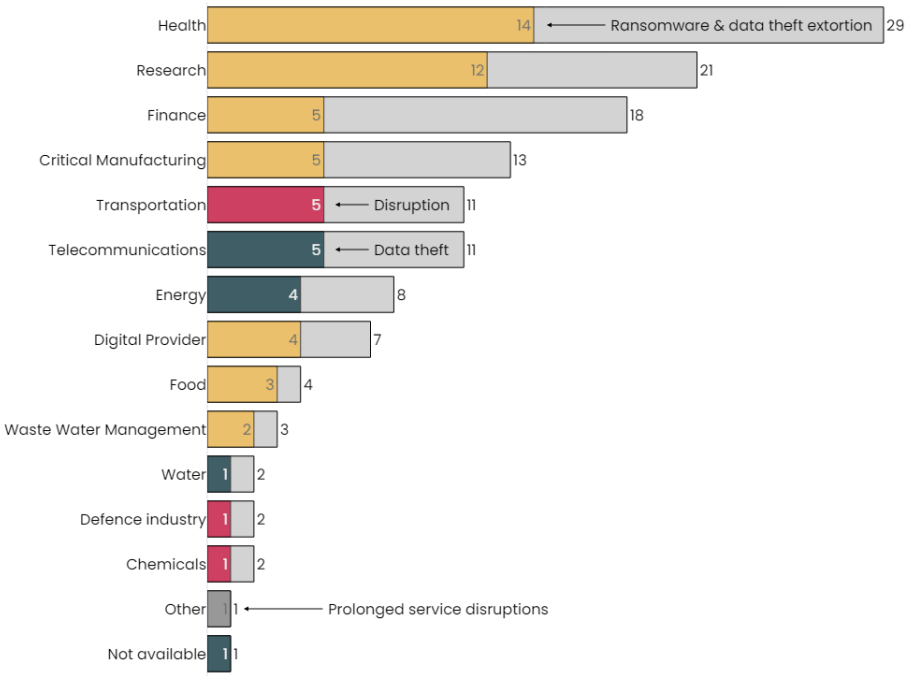
With a high concentration of organizations with low disruption tolerance and a duty of care for sensitive data, the health sector experienced ransomware attacks and data theft extortion.

State-sponsored intrusions tied to China nexus groups Volt Typhoon and Salt Typhoon consolidated as dominating concern for telecommunication providers in the US in 2024. While US intelligence assessments conclude that Volt Typhoon's behavior suggests efforts to prepare for operational disruptions, Salt Typhoon appears focused on data collection for intelligence and counter-intelligence purposes. These substantial differences in the group's suspected taskings underscore a differentiated interest by Chinese-affiliated actors in the telecom sector, that may expand further geographically.

These advanced persistent threats (APTs) have demonstrated capabilities that could easily be directed toward European targets, posing risks to the EU's critical infrastructure and data security. Geographical boundaries do not confine cyber threats. The tactics and tools employed by groups like Volt Typhoon and Salt Typhoon can be adapted to target organizations worldwide. The EU's interconnected digital infrastructure makes it susceptible to similar espionage and disruption activities. Given the strategic importance of telecommunications, European providers could be attractive targets for state-sponsored cyber actors. The breaches in the U.S. involved accessing sensitive communications data

and exploiting network vulnerabilities, tactics that could be replicated against EU telecom networks.

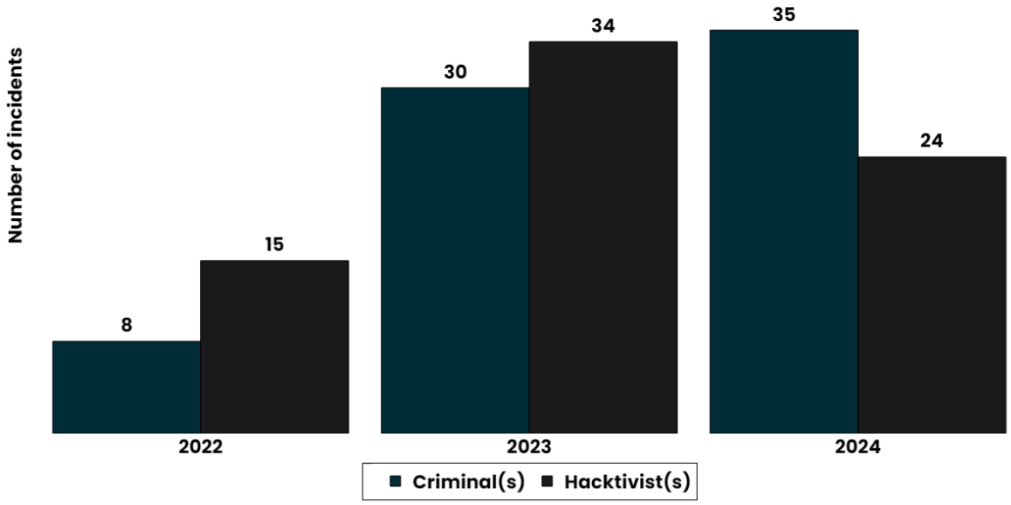
Across the EU, publicly reported activity predominantly pointed to criminally motivated data theft as the leading threat for the telecommunications sector.



Incidents targeting critical infrastructure sectors across EU member states, by volume and dominant operation type, 2024

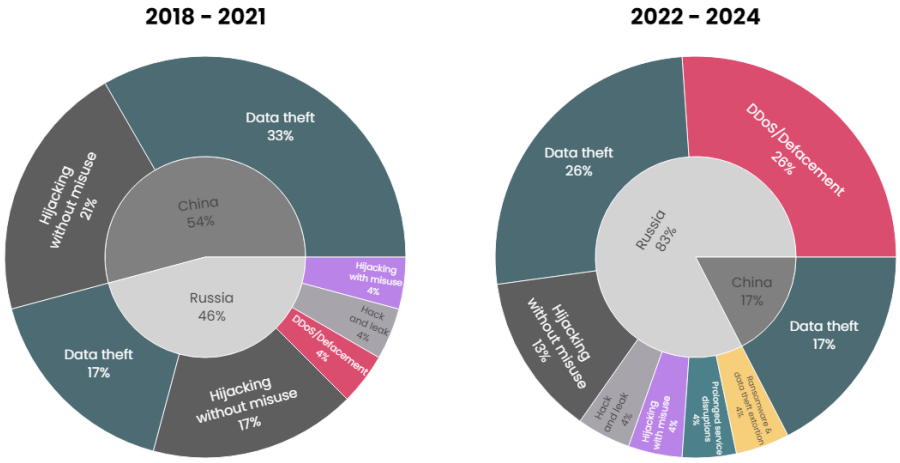
Two tales of tension: Disruption and stealth as operating principles of Russia and China nexus actors

The period since 2022 has coincided with an increase in the intensity of political conflicts, against which the Repository benchmarks tracked cyber operations. In particular for political conflicts involving state actors with advanced cyber capabilities and networked dependencies, this shift has contributed to a permissible operational environment, including for criminal and hacktivist activity, over the period of 2022-2024. (The Repository documents a subset of criminal and hacktivist activity directed against political organizations and critical infrastructure targets. On a case-by-case basis, this scope includes operations conducted in support of state actors or are directly addressed by public officials.)



Incidents by criminal and hacktivist groups targeting EU member states, 2022-2024

Changes in political restraint regarding the use of cyber capabilities appeared to influence the type of operation in which state-nexus actors affiliated with Russia and China engaged.



Operations by Russian and Chinese state nexus actors targeting EU member states, by operation type, 2018-2021 and 2022-2024

Since 2022, Russia-linked actors noticeably prioritized disruptive operations. This trend applies both to low-cost-high-visibility activities, such as DDoS attacks, as well as attempts

at prolonged system outages. Of particular concern, with regard to the latter, are capability developments within Russia's military intelligence service GRU, notably Unit 29155.

Operations of Unit 29155 trace back to at last 2008 and have focused on hybrid activities aimed at destabilizing EU and NATO member states, including the assassination attempts against a Bulgarian weapons dealer and the former GRU intelligence officer Sergei Skripal as well as explosions at Czech ammunition depots in 2014.

Around 2020, Unit 29155 expanded its scope, standing up a team for offensive cyber operations. Among its early activities, the Unit compromised three Estonian government ministries in November 2020. Estonia officially attributed the intrusion, which facilitated the theft of thousands of confidential documents, to the group in September 2024.

The group's destructive cyber activities gained attention following its involvement in deploying the WhisperGate wiper against Ukrainian targets shortly before Russia's assault in February 2022.

A joint advisory by four of the Five Eyes and six European partners released together with Estonia's attribution statement in September 2024 confirmed this shift in the group's cyber activities towards critical infrastructure targets. These findings document the Unit's use and preparation to use disruptive capabilities against organizations in the energy, transportation, and healthcare sector, as well as entities providing government and financial services of NATO allies and EU member states.

China nexus actors by comparison maintained a focus on espionage operations further emphasizing stealth, seemingly in an effort to avoid discovery and manage geopolitical tensions. State-affiliated groups frequently seek to relay operations through botnets and infiltrate target organizations through vulnerabilities in edge devices that offer limited monitoring capabilities.

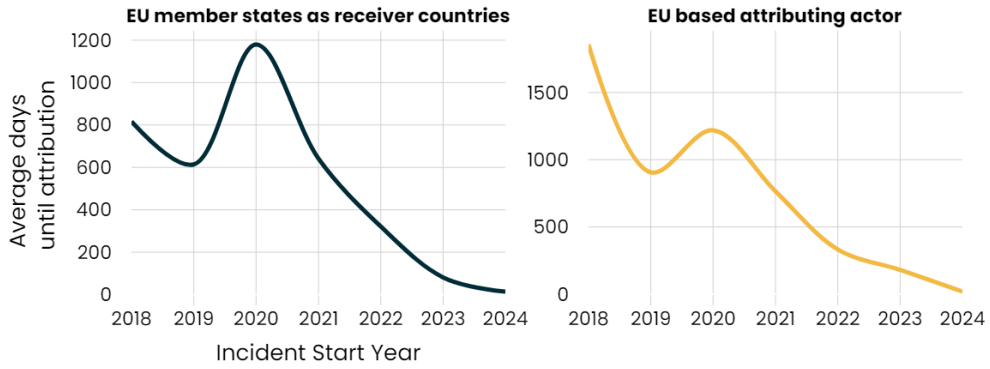
Operations specifically tracked for targets in EU member states likely underreport EU victimization, given that public reporting on China-associated campaigns does not always address the victimology distribution by geography in sufficient detail. Reports vary in their granularity, complicating a systematic distinction between European countries and EU member states. For the period 2022-2024, for instance, the Repository documented twice as many China nexus operations against targets in Europe than for EU member states.

At the global level, 13 times as many operations were observed for Chinese state-affiliated actors during the same period. Supporting reporting in early 2025 makes it likely that some campaigns, including reconnaissance activities linked to Flax Typhoon, also targeted critical infrastructure organizations in EU member states.

Attribution timelines are shrinking

Attribution time, as a measure for the period between an initial compromise and public information about the responsible, has notably and continuously decreased since 2020 for incidents tracked by the Repository.

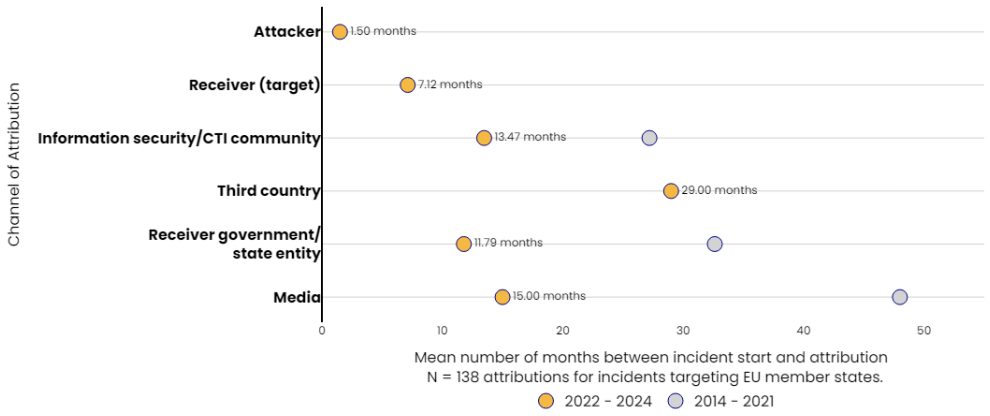
This acceleration of attribution timelines can be observed both for activities attributed directly attributed by an EU-based actor and for incidents affecting EU targets. The broader second measure also considers assessments of third countries and reports by threat intelligence companies based outside of the Union.



Average number of days between initial compromise and public attribution statements for incidents targeting EU member states, 2018-2024 | for all attribution statements recorded (left), for attribution statements from EU based actors (right)

While generally a positive development that contributes to greater public awareness about the sponsors of malicious activity, this downward trend also points to dynamics that are cause for caution. The reduction in attribution time is in part accounted for by the incentives for hacktivist and ransomware groups to promote and potentially exaggerate their activities. Criminal groups running extortion schemes, as part of their business model, advertise their compromises to increase public pressure on companies to comply with demands. Hacktivists or state-sponsored resort to similar tactics in the attempt to instill a sense of being under attack in target populations.

Within the EU, groups with pro-Russian targeting patterns stand out for their engagement in DDoS campaigns, as low-cost attempts to play to these psychological effects. Albeit regularly of negligible operational relevance, the high public visibility of short-lived access disruptions to websites contributes to disproportionate reporting by mainstream media that lack the capacity to evaluate the actual impact. Several such instances are recorded for 2024. In particular, activities of NoName057(16) and Anonymous Sudan drew widespread news coverage, including for the targeting of Belgian governmental websites as well as efforts to overwhelm the resources connected to DINUM, which manages the digital backbone of e-government services in France.

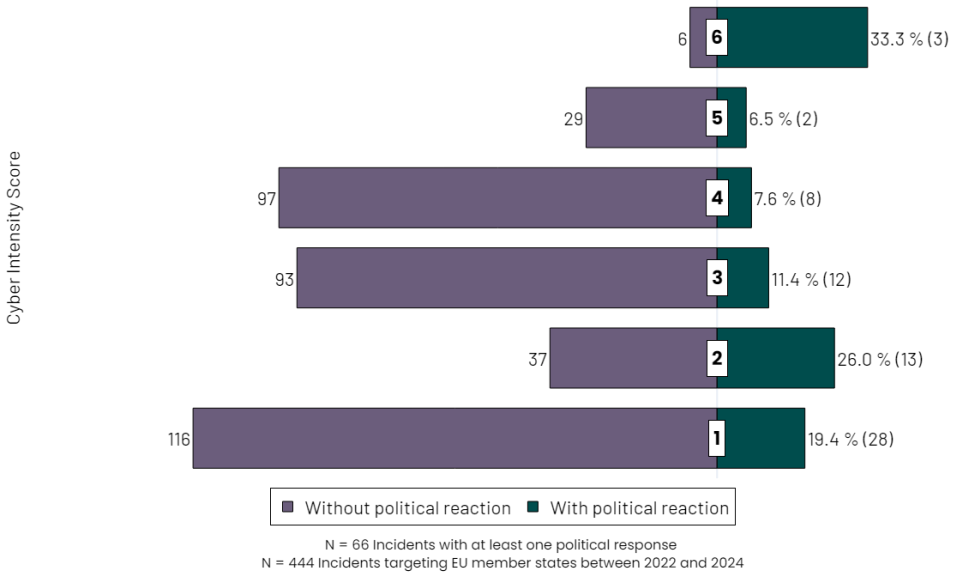


A further unpacking of attribution time by source of attribution reveals a convergence between threat intelligence community, predominantly represented by industry in the dataset, and government agencies. Underwriting the overarching drop in attribution time, this trend also indicates closer public-private coordination on the reporting of threat activities.

Political responses emphasize low- and high-intensity incidents

Challenging intuitive assumptions, a comparison of political responses based on the intensity of incidents does not indicate a linear increase in the response rate for operations with higher intensity.

The tracking of political responses considers a wide spectrum of cooperative, stabilizing, and preventive measures – such as capacity building assistance, diplomatic protest notes, or statements by public officials (including declarations by the High Representative at the EU level).



Distribution of incidents targeting EU members with and without political responses based on weighted incident intensity, 2022-2024

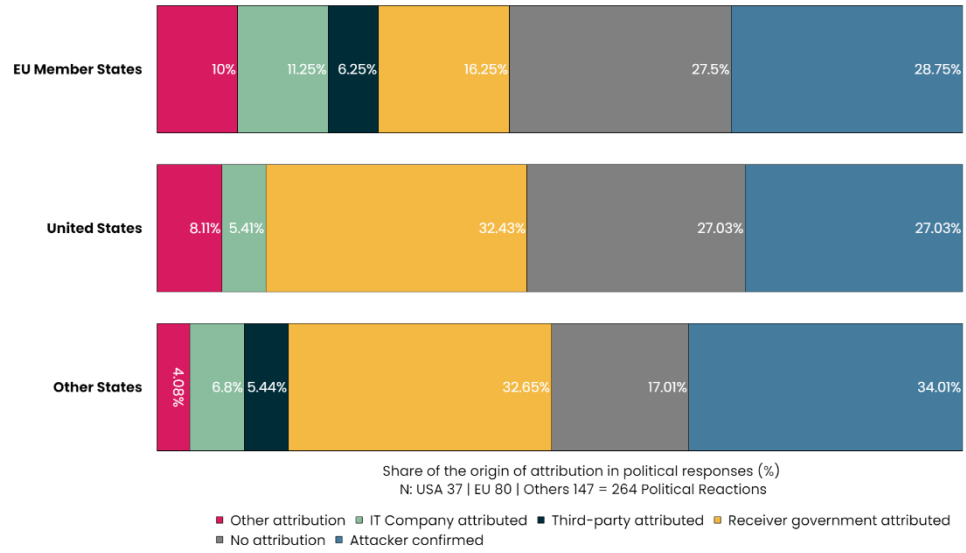
Responses are prevalent for incidents in the low-intensity categories 1 (19.4%) and 2 (25.5%). Among these incidents are easily publicly detected operation types, such as briefly successful DDoS attacks against the websites of public institutions. Despite being regularly short-lived in their effects against the targeted organizations, the visibility of these incidents encourage official responses with the aim to reassure populations. Events in 2024 demonstrated the importance of coherent communication strategies, to avoid the inadvertent inflation of threat perceptions in this effort. Initial statements by the French prime minister's office addressing the DDoS campaign launched by Anonymous Sudan against DINUM, for instance, categorized the incident as a cyber attack of "unprecedented

intensity". Subsequent, more measured media reports described this characterization as an exaggeration, citing an unnamed source within the French cybersecurity agency ANSSI.

Political responses regain in frequency at the high-intensity side of the scale, accounting for 33.3% of category 6 incidents. By contrast, the majority of incidents that make up the middle ground receives comparatively less public political attention at the level of individual operations. Activities in this intensity segment instead tend to be addressed through initiatives that seek to develop mitigations for an overall phenomenon, such as ransomware.

Legal responses remain tied to attribution timelines

An evaluation of political responses shows that responses by EU member states to malicious activity are not inherently contingent on earlier public attribution findings. For more than a quarter of tracked political responses (27.5%) EU member states proved willing to call out malicious behavior in the absence of a public track record of responsibility.



Political responses of state actors to incidents based on the supporting attribution source, 2022-2024

Actions under the EU's Cyber Diplomacy Toolbox, however, consider attribution the sovereign prerogative of member states. In accordance with this premise, all four sanction packages the EU had adopted by 2024 were based on previous public attribution findings by EU member states and third countries. This pattern holds going into 2025, as the Union imposed new sanctions against three officers of GRU Unit 29155 on 27 January over their involvement in the 2020 espionage campaign against Estonia.

Following almost four years later, Estonia's formal public attribution of the activity in September 2024 indicates that the general downward trend in attribution time does not preclude prolonged deliberations in individual cases. As the instance marked the first time Estonia officially attributed a cyber operation to a foreign state, both the testing of govern-

ment processes to coordinate attribution and the decision to combine attribution with additional legal measures to seek consequences may have contributed to the longer timeline. As a result of an international investigation with ten partners, Estonia's Prosecutor's Office on the same day declared that it had issued an arrest warrant for the same three GRU members later sanctioned by the EU. This announcement was further timed with the unsealing of US charges against five members of the unit and one civilian supporting its activities. The indictment of a civilian supporter points to practices within the group, identified by the FBI, to tasks cyber criminals to assist in its operations.

Despite their focus on espionage activity, the EU's latest round of restrictive measures on Unit 29155 appears to be part of a broader effort. The timing, calling out the group more than four years after the compromises of Estonian government networks, signals that more recent Russian sabotage efforts within the EU and partner countries are under scrutiny. In particular, the group's targeting of critical infrastructure and tactics to blend in with criminal activity correspond to the wider operational trends observed for 2024.

About the authors

Jakob Bund is an Associate at the German Institute for International and Security Affairs (SWP), where he serves as threat intelligence liaison for EuRepoC and editor of the Cyber Conflict Briefing series. Jakob is also a Senior Researcher for Cyber Conflict and Statecraft at Virtual Routes (formerly the European Cyber Conflict Research Initiative (ECCRI)).

Dr. Annegret Bendiek is Co-Lead of the Cluster "Cybersecurity and Digital Policy" and Senior Fellow in the EU/Europe Research Division at the German Institute for International and Security Affairs (SWP Berlin). Annegret serves as one of the principal investigators of EuRepoC.

Jonas Hemmelskamp, MA – Chief Data Scientist for the EuRepoC project and a PhD student at the Institute of Political Science, UHEI. He completed his master's degree in political science at Heidelberg University, where his thesis examined hybrid threat indicators.

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 Allianz SE.

EuRepoC provides updates on new entries in the Repository in a daily curated cyber incident tracker, which is openly available for subscription.

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3–4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org