Arbeitspapier

Arbeitspapiere sind Online-Veröffentlichungen der Forschungsgruppen. Sie durchlaufen kein förmliches Gutachterverfahren wie SWP-Studie, SWP-Aktuell und SWP-Zeitschriftenschau.

FORSCHUNGSGRUPPE EU / EUROPA | AP NR. 04, FEBRUAR 2025

Cyber Activity Balance 2024: Die Europäische Union im Fokus

Jakob Bund, Annegret Bendiek und Jonas Hemmelskamp

Die anhaltend hohe Bedrohungslage im Cyber- und Informationsraum stellt die Reaktionsstrategien europäischer Regierungen auf die Probe. Dabei stehen besonders europäische Ziele mitunter im Fokus von Cyberaktivitäten. Jahr um Jahr steigt die **Bedrohungsaktivität im Cyber- und Informationsraum** – auch in der Europäischen Union. Für das Jahr 2023 dokumentierte das **European Repository of Cyber Incidents** (EuRepoC) bereits einen Anstieg. Nach Beobachtungen der vorliegende Cyber Activity Balance[1] blieben die Aktivitäten auch im vergangenen Jahr auf einem erhöhten Niveau. Die **Operationen gegen EU-Ziele** nahmen um 16 Prozent zu. In Anbetracht des leichten Rückgangs des Volumens der weltweit verfolgten Operationen (ohne EU-Mitgliedstaaten) um 6,3 Prozent deutet diese Entwicklung auf eine **Konzentration böswilliger Aktivitäten** gegen EU-Ziele im Jahr 2024 hin.

Unter den für 2024 erfassten Operationen weisen Ransomware-Aktionen, die durch die Verschlüsselung oder den Diebstahl von betriebswichtigen Daten weitreichendes Schadenspotential aufbauen, die stärkste Intensität auf, sowohl für Ziele innerhalb der EU als auch weltweit. Für **Organisationen der Kritischen Infrastruktur** und der Politik blieben die mit Ransomware verbundenen Bedrohungen auf einem ähnlichen Niveau wie 2023, wobei ein geringfügiger Anstieg bei leicht abnehmender Intensität zu beobachten ist.

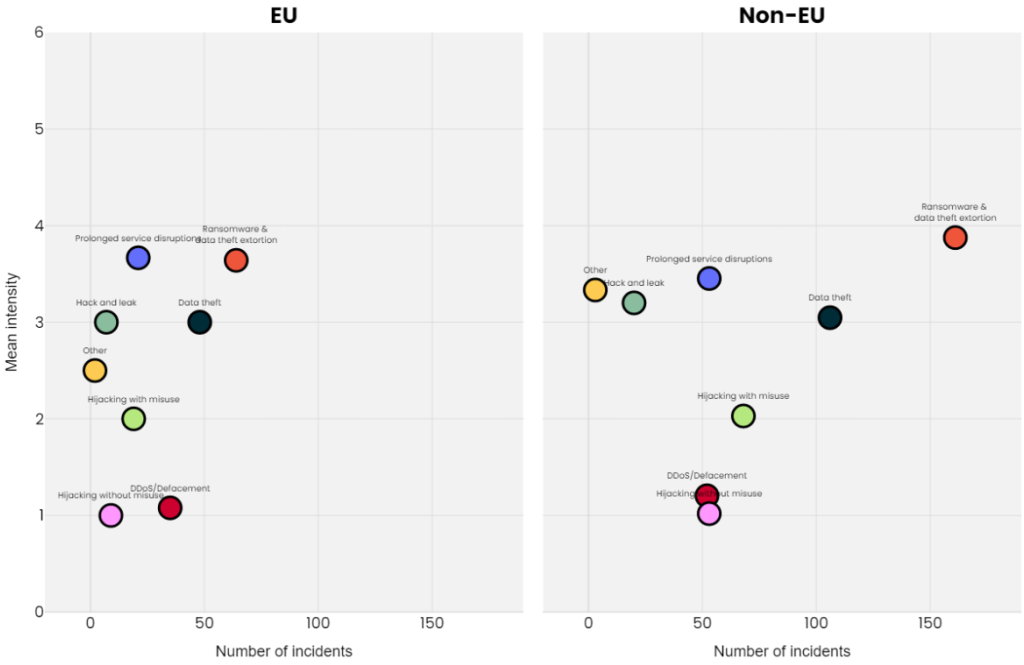
Die unveränderte **Intensität von Cyberangriffen** spiegelt die Störungen wider, die Ransomware weiterhin verursacht, auch wenn die Anzahl und Höhe der Lösegeldzahlungen im Jahr 2024 einigen Quellen zufolge zurückgegangen ist. Das Blockchain-Analyseunternehmen Chainalysis brachte diese Erkenntnisse mit den Erfolgen der Strafverfolgungsbehörden im Jahr 2024 in Verbindung, die kriminelle Netzwerke zerschlugen, Lösegeldzahlungen zurückführten und betroffenen Organisationen Entschlüsselungsmöglichkeiten zur Verfügung stellten. Dies stellt angesichts der anhaltend hohen Anzahl von Ransomware-Angriffen einen **wirkungsvollen Durchbruch** dar.

Debatte über das Verbot von Lösegeldzahlungen

Nach einer globalen Bilanzierung durch das Cybersicherheitsberatungsunternehmen NCC Group stellten die 5236 registrierten Angriffe im Jahr 2024 die größte Anzahl seit Beobachtungsbeginn durch das Unternehmen im Jahr 2021 dar. Trotz des **international koordinierten Schlags gegen LockBits Infrastruktur** Anfang 2024 zeigen NCC-Statistiken, dass die Gruppe bei einem Anteil von 10 Prozent für mehr Vorfälle verantwortlich war als jeder andere Akteur.

Ob die 2024 beobachteten Veränderungen im Zahlungsverhalten der Opfer das Zielmuster von Ransomware-Gruppen beeinflussen werden, bleibt ein wichtiger Analysepunkt, insbesondere angesichts von Vorschlägen, **Lösegeldzahlungen zu verbieten** oder eine Meldepflicht einzuführen, wie durch Konsultationen des britischen **National Cyber Security Centres** im Januar 2025 angeregt.

[1] Die Cyber Activity Balance ist Teil der Cyber Conflict Briefing Reihe, einem analytischen Produkt von EuRepoC. Die deutsche Ausgabe der Cyber Activity Balance 2024 ist in Zusammenarbeit mit Tagesspiegel Background - Cybersecurity erschienen. Eine englische Version ist parallel als EuRepoC-Bericht erschienen.



Anzahl und Intensität der Vorfälle nach Art der Operation, 2024

Ransomware und Erpressung durch Datendiebstahl stellen nach wie vor eine **sektorübergreifende Bedrohung.** Diese anhaltende Problematik erklärt sich unter anderem durch die opportunistischen Angriffspraktiken krimineller Gruppen, die versuchen, Schwachstellen auszunutzen, wo immer sie sie finden. Unter Organisationen den Kritischen Infrastrukturen innerhalb der EU war der **Gesundheitssektor am häufigsten betroffen**. Die geringe Toleranz für Ausfälle in der Patientenversorgung und die besonderen Sorgfaltspflichten für den Umgang mit medizinischen Daten machen gerade Organisationen im Gesundheitsbereich anfällig für Ransomware-Angriffe und Erpressungen durch Datendiebstahl.

Kritische Infrastruktur im Fokus

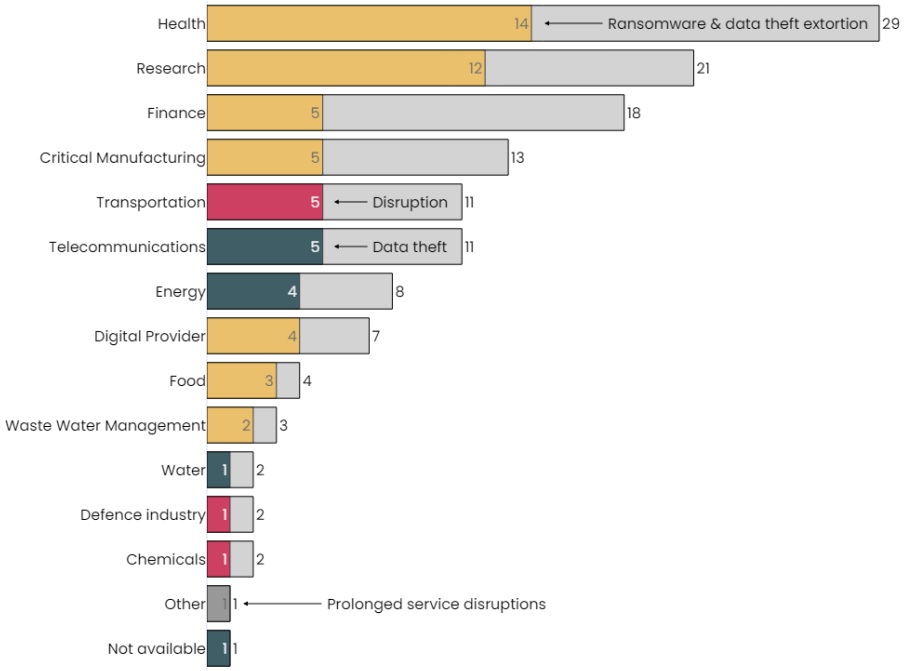
Staatlich geförderte Angriffe, die mit den **chinesischen Nexus-Gruppen „Volt Typhoon“ und „Salt Typhoon“** in Verbindung stehen, beherrschten 2024 die Sicherheitslage von Telekommunikationsanbietern in den USA (Tagesspiegel Background berichtete). Während die US-Geheimdienste zu dem Schluss kommen, dass das Verhalten von Volt Typhoon auf Bemühungen hindeutet, sich auf **Betriebsstörungen vorzubereiten**, scheint sich Salt Typhoon auf die **Datenerfassung zu nachrichtendienstlichen Zwecken** zu konzentrieren. Diese erheblichen Unterschiede in den mutmaßlichen Aufgaben der Gruppe unterstreichen das differenzierte Interesse chinesischer Akteure am Telekommunikationssektor.

Diese professionellen Bedrohungsakteure (APTs) haben Fähigkeiten unter Beweis gestellt, die sich **leicht** auch **auf europäische Ziele richten** lassen und Risiken für die Kritische Infrastruktur und die Datensicherheit der EU darstellen. Die Taktiken und Werkzeuge, die von Gruppen wie Volt Typhoon und Salt Typhoon eingesetzt werden, können an Organisationen auf der ganzen Welt angepasst werden. Die vernetzte digitale Infrastruktur der EU macht sie **anfällig für ähnliche Spionage- und Störungsaktivitäten**. Ange-

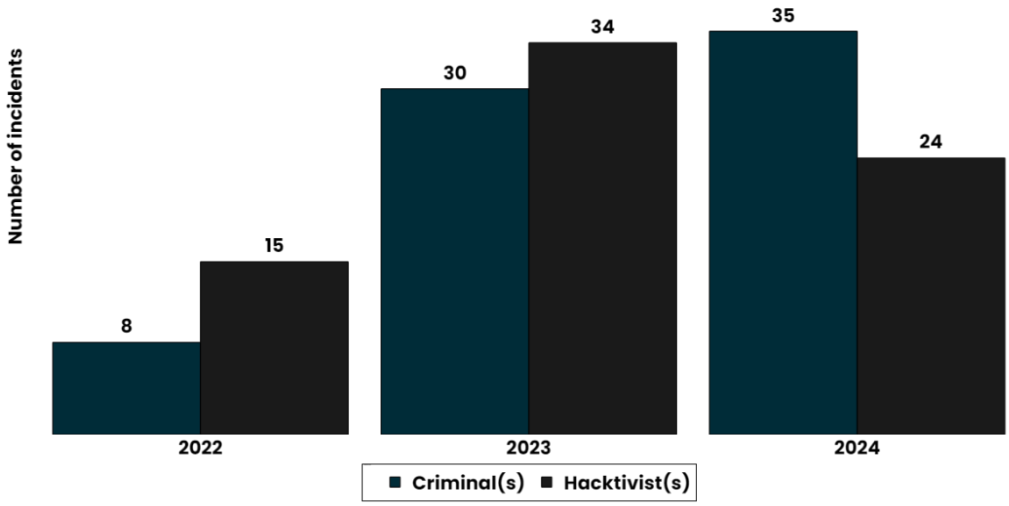
sichts der **strategischen Bedeutung der Telekommunikation** könnten europäische Anbieter attraktive Ziele für staatlich geförderte Cyberakteure sein. Bei den Sicherheitsverletzungen in den USA ging es um den Zugriff auf sensible Kommunikationsdaten und die **Ausnutzung von Netzwerkschwachstellen** – Taktiken, die auch gegen Telekommunikationsnetze in der EU angewendet werden könnten. In der gesamten EU deuteten öffentlich gemeldete Aktivitäten überwiegend auf **kriminell motivierten Datendiebstahl** als größte Bedrohung für den Telekommunikationssektor hin.

Intensität nimmt weiter zu

Seit 2022 hat die **Intensität politischer Konflikte** zugenommen, an denen staatliche Akteure mit weit entwickelten Cyberfähigkeiten und vernetzten Abhängigkeiten beteiligt sind. Diese Spannungen schaffen Freiräume auch für kriminelle und hacktivistische Aktivitäten.

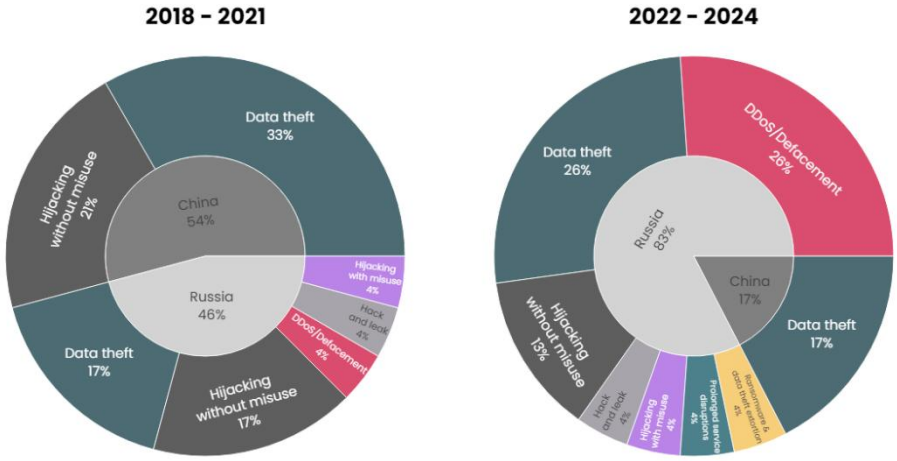


Vorfälle, die auf kritische Infrastruktursektoren in den EU-Mitgliedstaaten abzielen, nach Umfang und vorherrschender Art der Operation, 2024



Vorfälle durch kriminelle und hacktivistische Gruppen, die gegen EU-Mitgliedstaaten gerichtet sind, 2022–2024

Dabei scheint auch die **schwindende politische Zurückhaltung** in Bezug auf den Einsatz von Cyberfähigkeiten die Art der Operationen zu beeinflussen, an denen Akteure mit Bezug zu Russland und China beteiligt waren.



Operationen von Akteuren mit staatlichem Bezug aus Russland und China, die auf EU-Mitgliedstaaten abzielen, nach Art der Operation, 2018–2021 und 2022–2024

Seit 2022 haben mit Russland verbundene Akteure **deutlich erkennbar** den Schwerpunkt Richtung Störmaßnahmen verlagert. Dieser Trend gilt sowohl für **kostengünstige Aktivitäten mit hoher Sichtbarkeit**, wie DDoS-Angriffe, als auch für Versuche, Systemausfälle über einen längeren Zeitraum zu verursachen. Besonders besorgniserregend sind in diesem Zusammenhang die Fähigkeitsentwicklungen innerhalb des russischen Militärgeheimdienstes GRU, unter anderem durch die **Einheit 29155**.

29155: Hybride Operationen und offensive Cyberaktivitäten

Operationen der Einheit 29155 reichen bis mindestens 2008 zurück und konzentrierten sich auf **hybride Aktivitäten**, die darauf abzielten, EU- und Nato-Mitgliedstaaten zu destabilisieren, darunter die Mordanschläge auf einen bulgarischen Waffenhändler und den ehemaligen GRU-Geheimdienstoffizier Sergei Skripal sowie Anschläge auf tschechische Munitionsdepots im Jahr 2014.

Um das Jahr 2020 erweiterte die Einheit 29155 ihren Aufgabenbereich und stellte ein **Team für offensive Cyberoperationen** auf. Zu den ersten Aktivitäten der Einheit gehörte die Kompromittierung von drei estnischen Ministerien im November 2020. Estland machte die Gruppe allerdings erst im September 2024 offiziell für den Einbruch verantwortlich, der den Diebstahl tausender vertraulicher Dokumente zur Folge hatte. Die **zerstörerischen Cyberaktivitäten** der Gruppe erregten Aufmerksamkeit, nachdem sie kurz vor dem russischen Angriff im Februar 2022 am Einsatz des „WhisperGate"-Wipers gegen ukrainische Ziele beteiligt war.

Ein gemeinsamer Bericht von vier der Five-Eyes-Staaten und sechs europäischen Partnern, der zusammen mit der Attribuierung Estlands im September 2024 veröffentlicht wurde, bestätigte diese **Verlagerung der Cyberaktivitäten** der Gruppe auf Ziele Kritischer Infrastrukturen. Diese Erkenntnisse dokumentieren den Einsatz und die Vorbereitung der Einheit auf den **Einsatz von Störfähigkeiten** gegen Organisationen im Energie-, Transport- und Gesundheitssektor sowie gegen Einrichtungen, die Regierungs- und Finanzdienstleistungen von Nato-Verbündeten und EU-Mitgliedstaaten erbringen.

Chinesische Akteure setzen auf Spionage

Im Vergleich dazu konzentrierten sich die **Akteure mit China-Nexus** weiterhin auf **Spionageoperationen**, unter erhöhten Anstrengungen ihre Aktivitäten zu maskieren, mutmaßlich in dem Bestreben, nicht entdeckt zu werden und politische Spannungen zu vermeiden. Solche staatlich unterstützte Gruppen versuchen häufig, Operationen über Botnets zu leiten und Zielorganisationen über Schwachstellen in Edge-Geräten zu infiltrieren, die nur begrenzte Überwachungsmöglichkeiten bieten.

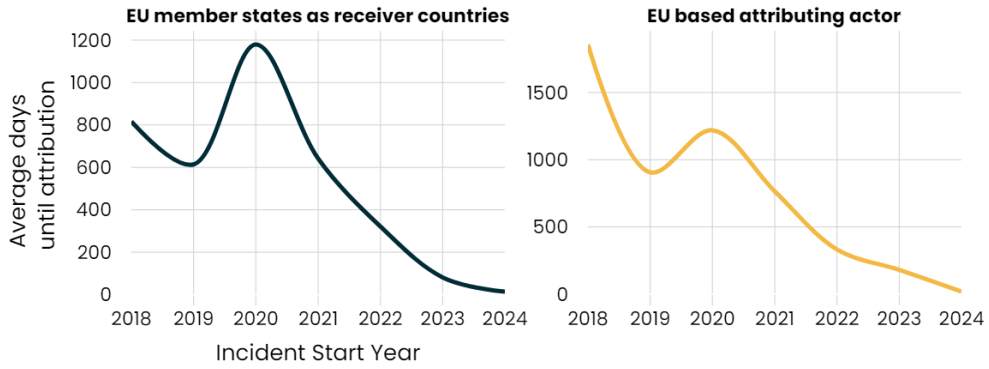
Bei **Operationen**, die speziell auf **Ziele in EU-Mitgliedstaaten ausgerichtet** sind, wird die Viktimisierung in der EU wahrscheinlich untererfasst, da in der öffentlichen Berichterstattung über mit China in Verbindung stehende Kampagnen die geografische Verteilung der Opfer nicht immer ausreichend detailliert behandelt wird. Die Berichte variieren in ihrer Granularität, was eine systematische Unterscheidung zwischen europäischen Ländern und EU-Mitgliedstaaten erschwert. Für den Zeitraum 2022–2024 dokumentierte das Repository beispielsweise **doppelt so viele Operationen mit China-Bezug** gegen Ziele in Europa wie gegen EU-Mitgliedstaaten.

Auf globaler Ebene wurden im selben Zeitraum **dreizehnmal** so viele Operationen von mit dem chinesischen Staat verbundenen Akteuren beobachtet. Die Berichterstattung Anfang 2025 lässt vermuten, dass einige Kampagnen, darunter auch Aufklärungsaktivitäten im Zusammenhang mit „Flax Typhoon“, auch auf Organisationen für Kritische Infrastruktur in EU-Mitgliedstaaten abzielten.

Attributionszeit nimmt ab – ein Erfolgszeichen?

Die Zuordnungszeit als Maß für den **Zeitraum** zwischen einer **ersten Kompromittierung** und der **Veröffentlichung von Informationen** über die Verantwortlichen hat sich seit 2020 für die vom Repository erfassten Vorfälle deutlich und kontinuierlich verringert.

Diese **Verkleinerung** der Attributionszeiträume ist sowohl bei Aktivitäten, die von einem in der EU ansässigen Akteur zugeordnet wurden, als auch bei Vorfällen, die EU-Ziele betreffen, festzustellen. Die breit gefassten letzteren Beobachtungen berücksichtigen auch Bewertungen von Drittländern und Berichte von Threat-Intelligence-Unternehmen mit Sitz außerhalb der EU.



Durchschnittliche Anzahl der Tage zwischen dem ersten Angriff und öffentlichen Zuschreibungserklärungen für Vorfälle, die sich gegen EU-Mitgliedstaaten richten, 2018–2024 | für alle erfassten Zuschreibungserklärungen (links), für Zuschreibungserklärungen von Akteuren mit Sitz in der EU (rechts)

Obwohl dies im Allgemeinen eine positive Entwicklung ist, die zu einer stärkeren Sensibilisierung der Öffentlichkeit für die Verantwortlichen böswilliger Aktivitäten beiträgt, deutet dieser **Abwärtstrend** auch auf eine **Dynamik** hin, die **zur Vorsicht** mahnt.

Die **Verkürzung** der Attributionszeit ist zum Teil auf die **Anreize** für Hacktivisten und Ransomware-Gruppen zurückzuführen, ihre Aktivitäten zu bewerben und möglicherweise zu übertreiben. Kriminelle Gruppen, die im Rahmen ihres Geschäftsmodells auf Erpressung setzen, machen ihre Kompromittierungen öffentlich, um den **öffentlichen Druck auf Unternehmen zu erhöhen**, ihren Forderungen nachzukommen. Hacktivisten oder staatlich geförderte Gruppen greifen auf ähnliche Taktiken zurück, um in der breiten Bevölkerung ein Gefühl der Unsicherheit zu erwecken.

Störaktionen mit hoher medialer Reichweite

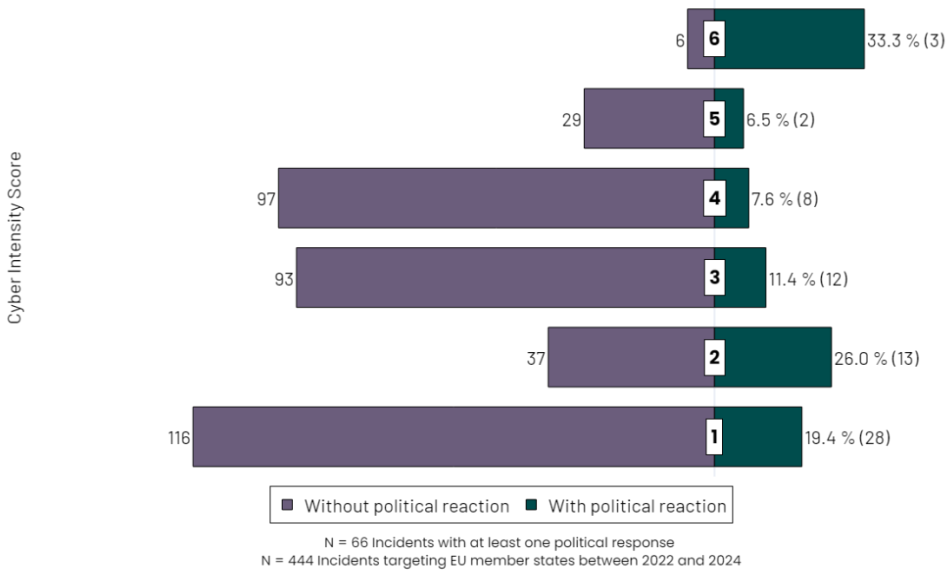
Innerhalb der EU zeichnen sich Gruppen mit prorussischen Angriffsmustern durch ihr Engagement in DDoS-Kampagnen aus. Obwohl sie regelmäßig von **vernachlässigbarer operativer Relevanz** sind, trägt die hohe öffentliche Sichtbarkeit **kurzlebiger Zugriffsstörungen** auf Webseiten zu einer **unverhältnismäßigen Berichterstattung** durch die Mainstream-Medien bei, denen die Kapazitäten fehlen, um die tatsächlichen Auswirkungen bewerten zu können. Für 2024 sind mehrere solcher Fälle verzeichnet. Insbesondere die Aktivitäten von „NoName057(16)“ und „Anonymous Sudan“ sorgten für eine **breite Berichterstattung** in den Nachrichten, unter anderem über die **Angriffe auf belgische Regierungswebseiten** sowie über die Bemühungen das Dinum, das den digitalen Backbone der E-Government-Dienste in Frankreich verwaltet, zu überlasten.

Eine weitere Aufschlüsselung der Attributionszeit nach Zuordnungsquelle zeigt eine Annäherung zwischen der Threat Intelligence Community, die im Datensatz überwiegend durch die Industrie vertreten ist, und Regierungsbehörden. Dieser Trend, der den **generellen Rückgang der Attributionszeit** untermauert, deutet auch auf eine **engere öffentlich-private Koordinierung** in der Berichterstattung von Bedrohungsaktivitäten hin.

Ein Vergleich der politischen Reaktionen auf der Grundlage der Intensität der Vorfälle, deutet erstaunlicherweise nicht auf eine **lineare Zunahme der getroffenen Gegenmaßnahmen hin.** Das heißt: Cyberangriffe mit höherer Intensität lösen nicht äquivalent zu ihrer Intensität diplomatische, politische oder rechtliche Gegenreaktionen aus.

Kohärente Kommunikation als entscheidender Faktor

Politische Reaktionen sehen grundsätzlich ein **breites Spektrum** an kooperativen, stabilisierenden und präventiven Maßnahmen vor – wie zum Beispiel die Unterstützung beim Kapazitätsaufbau, diplomatische Protestnoten oder Erklärungen von Amtsträgern (einschließlich Erklärungen des Hohen Vertreters auf EU-Ebene).



Verteilung von Vorfällen, die sich gegen EU-Mitglieder richten, mit und ohne politische Reaktionen auf der Grundlage der gewichteten Vorfallsintensität, 2022–2024

Reaktionen sind bei Vorfällen in den Kategorien mit geringer Intensität 1 (19,4 Prozent) und 2 (25,5 Prozent) weit verbreitet. Zu diesen Vorfällen gehören leicht öffentlich erkennbare Arten von Operationen, wie etwa kurzzeitig erfolgreiche DDoS-Angriffe auf die Webseiten öffentlicher Einrichtungen. Obwohl die Auswirkungen dieser Vorfälle auf die Zielorganisationen in der Regel **nur von kurzer Dauer** sind, sorgt die **Sichtbarkeit** dieser Vorfälle für eine auffällig hohe Zahl an offiziellen Reaktionen mit dem Ziel, die Bevölkerung zu beruhigen.

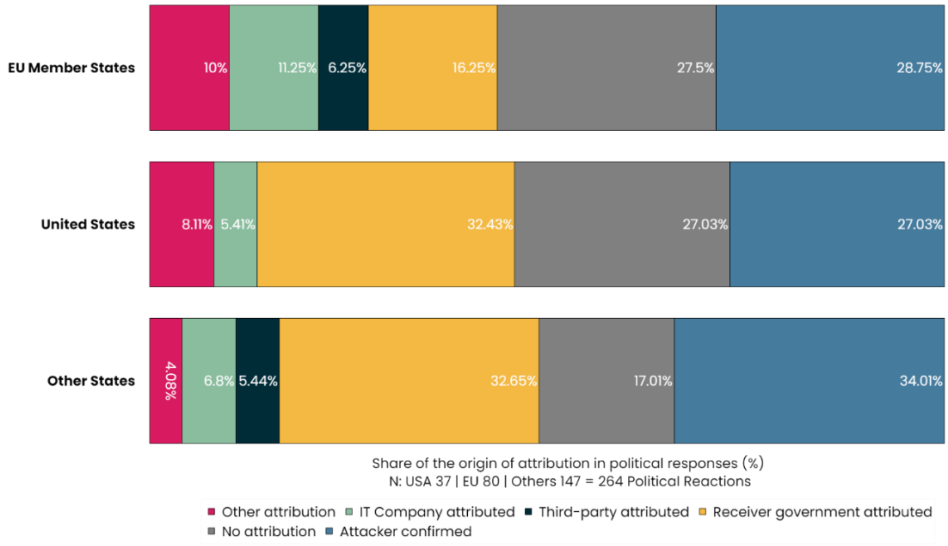
Die Ereignisse im Jahr 2024 haben gezeigt, wie wichtig **kohärente Kommunikationsstrategien** sind, um bei diesen Bemühungen eine **unbeabsichtigte Zuspitzung** der Bedrohungswahrnehmung zu vermeiden. In ersten Stellungnahmen des Büros des französischen Premierministers zur DDoS-Kampagne, die von Anonymous Sudan gegen Dinum lanciert wurden, wurde der Vorfall beispielsweise als Cyberangriff von „beispielloser Intensität" eingestuft. In späteren, abgewogeneren Medienberichten bezeichnete eine ungenannte Quelle innerhalb der französischen Cybersicherheitsbehörde ANSSI diese Charakterisierung als übertrieben.

Europäische Sanktionsmaßnahmen

Politische Reaktionen nehmen für Operationen mit hoher Intensität wieder zu und machen 33,3 Prozent der Vorfälle der Kategorie 6 aus. Im Gegensatz dazu erhält der mittlere Intensitätsbereich, der die **Mehrheit der Vorfälle** ausmacht, vergleichsweise weniger öffentliche politische Aufmerksamkeit. Aktivitäten in dieser Intensitätsstufe werden seltener auf der Ebene einzelner Operationen adressiert. Stattdessen werden breitangelegte, sektorübergreifende Herausforderungen, wie beispielsweise in der Ransomwarebekämpfung, vermehrt durch Initiativen angegangen, die **Abhilfemaßnahmen** im größeren Maßstab auf den Weg zu bringen.

Eine Auswertung der politischen Reaktionen zeigt auch, dass die **Reaktionen der EU-Mitgliedstaaten** auf böswillige Cyberaktivitäten nicht grundsätzlich von früheren öffentlichen Attributionen abhängig sind. Bei mehr als einem Viertel der erfassten politischen Reaktionen (27,5 Prozent) zeigten sich EU-Mitgliedstaaten auch ohne vorherige öffentliche Attribution bereit, Cyberangriffe zu verurteilen.

Maßnahmen desdiplomatischen Reaktionsrahmens **für Cyberdiplomatie** (Cyber Diplomacy Toolbox) betrachten die Zuschreibung als das souveräne Vorrecht der Mitgliedstaaten. Ausgehend von dieser Grundlage basierten alle vier **Sanktionspakete**, die die EU bis 2024 verabschiedet hatte, auf früheren öffentlichen Attributionen von EU-Mitgliedstaaten und Drittländern. Dieses Muster setzt sich auch im Jahr 2025 fort, mit den von der EU am 27. Januar verhängten **neuen Sanktionen** gegen drei Offiziere der GRU-Einheit 29155, die in die Spionagekampagne gegen Estland im Jahr 2020 verwickelt waren (Tagesspiegel Background berichtete).



Politische Reaktionen staatlicher Akteure auf Vorfälle auf der Grundlage der unterstützenden Zuschreibungsquelle, 2022–2024

Mit fast vier Jahren Abstand deutet die formelle öffentliche Zuschreibung der Aktivitäten durch Estland im September 2024 darauf hin, dass der allgemeine Abwärtstrend bei der Attributionszeit nicht ausschließt, dass **in Einzelfällen** längere Abwägungsprozesse notwendig sind. Da Estland in diesem Fall erstmals offiziell eine Cyberoperation einem ausländischen Staat zuschrieb, könnten sowohl die **Erprobung von Regierungsprozessen** zur Koordinierung der Verantwortungszuschreibung als auch die Entscheidung, die Zuschreibung mit zusätzlichen rechtlichen Maßnahmen zu begleiten, zu der längeren Zeitspanne in diesem speziellen Fall beigetragen haben.

Als Ergebnis einer internationalen Untersuchung mit zehn Partnern erklärte die estnische Staatsanwaltschaft zeitgleich, dass sie einen **Haftbefehl** gegen dieselben drei GRU-Mitglieder erlassen habe, die später von der EU sanktioniert wurden. Diese Ankündigung erfolgte zeitlich abgestimmt mit der Veröffentlichung in den Vereinigten Staaten einer Anklage von fünf Angehörigen der Einheit und einer weiteren Person, die deren Aktivitäten unterstützte. Die Anklage eines zivilen Unterstützers deckt sich mit Erkenntnissen des FBI über die Einbindung von Cyberkriminellen in die Operationen russischer Geheimdienste.

Trotz ihres **Schwerpunkts auf Spionageaktivitäten** scheint die jüngste Runde restriktiver Maßnahmen der EU gegen die Einheit 29155 Teil einer umfassenderen Anstrengung zu sein. Der Zeitpunkt, zu dem die Gruppe mehr als vier Jahre nach der Kompromittierung der estnischen Regierungsnetzwerke an die Öffentlichkeit gebracht wird, signalisiert eine verstärkte Aufmerksamkeit auf **neuere russische Sabotageversuche** innerhalb der EU und ihrer Partnerländer. Insbesondere die Ausrichtung der Gruppe auf Kritische Infrastrukturen und die Taktik, Fähigkeiten krimineller Akteure einzubeziehen, deuten auf eine Ausweitung des operativen Spektrums hin.

Über die Autoren

Jakob Bund ist Wissenschaftler an der Stiftung Wissenschaft und Politik (SWP), wo er insbesondere die operative Auswertung von Cyberbedrohungen für EuRepoC verantwortet. Daneben ist Jakob Senior Researcher für Cyber Conflict und Statecraft bei Virtual Routes (ehemals European Cyber Conflict Research Initiative (ECCRI)).

Dr. Annegret Bendiek ist Co-Leiterin des Clusters „Cybersicherheit und Digitalpolitik" und Senior Fellow in der Forschungsgruppe EU/Europa an der Stiftung Wissenschaft und Politik (SWP). Annegret ist eine der Principal Investigator des europäischen Forschungskonsortiums von EuRepoC.

Jonas Hemmelskamp ist Datenwissenschaftler für das EuRepoC-Projekt und Doktorand am Institut für Politikwissenschaft der Universität Heidelberg. Er schloss sein Masterstudium der Politikwissenschaft an der Universität Heidelberg ab, wo er sich in seiner Abschlussarbeit mit hybriden Bedrohungsindikatoren befasste.

Über EuRepoC

Das European Repository of Cyber Incidents ist ein europäisches Forschungsprojekt mit dem Ziel, Informationen und Wissen über Cyberkonflikte sichtbar zu machen. Es wird von der Universität Heidelberg in Zusammenarbeit mit der Universität Innsbruck, der Stiftung Wissenschaft und Politik und dem Cyber Policy Institute (Estland) geleitet und derzeit vom Auswärtigen Amt und der Allianz SE finanziert.

EuRepoC informiert in einem täglich kuratierten Cyber Incident Tracker über neue Einträge im Repository, der offen zur Anmeldung zur Verfügung steht.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

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