European
Repository of
Cyber Incidents

European Repository

Cyber Conflict Briefing

2025 CYBER ACTIVITY BALANCE

Die Europäische Union im Fokus

Lena Rottinger
Annegret Bendiek
Jonas Hemmelskamp

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

*Über die Autor*innen*

Lena Rottinger ist wissenschaftliche Mitarbeiterin im EuRepoC-Projekt und ist verantwortlich für die politische Kodierung von Cybervorfällen. Zuvor absolvierte sie ihr Masterstudium der Politikwissenschaft an der Universität Heidelberg und der Universität Bologna mit dem Schwerpunkt in den Internationalen Beziehungen. Ihre Forschungsinteressen liegen im Bereich (Cyber-) Sicherheitspolitik, Diplomatie und Theorien der Internationalen Beziehungen.

Dr. Annegret Bendiek ist Co-Leiterin des Clusters „Cybersicherheit und Digitalpolitik“ und Senior Fellow in der Forschungsabteilung EU/Europa an der Stiftung Wissenschaft und Politik (Berlin). Annegret ist eine der Hauptforscherinnen von EuRepoC.

Jonas Hemmelskamp ist Chief Data Scientist beim EuRepoC und Doktorand am Institut für Politische Wissenschaft der Universität Heidelberg. Er schloss sein Masterstudium der Politikwissenschaft an der Universität Heidelberg ab, wo er sich in seiner Masterarbeit mit Indikatoren für hybride Bedrohungen befasste.

linkedin/EuRepoC

contact@eurepoc.eu

https://eurepoc.eu

@eurepoc.bsky.social

About this report

Der „Cyber Conflict Briefing“ und der „Cyber Activity Balance“ sind Produkte, die von EuRepoC erstellt werden. Die deutsche Ausgabe erscheint in Zusammenarbeit mit **Tagesspiegel Background – Cybersecurity.**

Dieser Balance wurde im Rahmen des vom Auswärtigen Amt geförderten Projekts „Europäische Diplomatie und Normbildung. Potentiale für eine operative Cyber-Incidents- und Responseforschung heben“ (2026–2027) erstellt.

März 2026

Die Situation ist paradox – und problematisch

Im Januar 2026 stellte die Europäische Kommission ein umfassendes Cybersicherheitspaket vor. Es beinhaltet eine Überarbeitung des Cybersicherheitsgesetzes sowie gezielte Änderungen an der NIS-2-Richtlinie. Ein Ziel des Entwurfs ist, die Zusammenarbeit zwischen den Mitgliedstaaten zu verbessern, vor allem durch ein stärkeres operatives Mandat der Enisa. Durch die aktive Teilnahme am Csirt-Netzwerk und EU-Cyclone sowie die gemeinsame Entwicklung von Repositorien für Cyber-Bedrohungsinformationen mit anderen Behörden wie Europol soll die Enisa zu einem Ankerpunkt für ein gemeinsames europäisches Cyber-Lagebild (Situational Awareness) werden.

Die Initiative basiert auf drei zentralen Prämissen:

- Mehr Zusammenarbeit und Informationsaustausch ermöglichen der EU ein besseres Verständnis und proportionale Reaktionen auf Cyber-Bedrohungen.
- Das EU-Cyber-Lagebild vereinheitlicht die Risikoerfassung, trägt aber auch zur Rechtsangleichung bei Cyberangriffs-Bewertungen bei.
- Bestehende Koordinierungslücken lassen sich in erster Linie durch verbesserte operative Mechanismen schließen. Der Kommissionsentwurf geht auch davon aus, dass groß angelegte Vorfälle den eigentlichen Stresstest für die „europäische Solidarität“ (Art. 2 EUV) darstellen.

Diese Cyber Balance 2025 überprüft diese Annahmen mit den Daten des European Repository on Cyber Incidents (EuRepoC), die regelmäßig hier im Tagesspiegel Background Cybersecurity veröffentlicht werden. Die Ergebnisse zeigen ein komplexeres Lagebild, das die kumulative Wirkung von vielen einzelnen Cyberangriffen in den Blick nimmt. Während die Gesamtzahl der einzelnen Operationen, die auf EU-Länder abzielten, leicht zurückging, ist parallel die Zahl der betroffenen Organisationen gestiegen. Dies deutet darauf hin, dass sich in miteinander verbundenen Sektoren zunehmend kumulative und vermehrte Spill-over-Effekte bilden.

Gleichzeitig blieben einzelne Cybernetzwerkoperationen oft unterhalb der Schwelle der im EU-Rechtsakt definierten „groß angelegten“ Cybervorfälle, die jedoch durchaus aufgrund ihrer Kumulation als eine systemische (Über-)Belastung für die Stabilität und Funktionsweise der Europäischen Union eingeordnet werden könnten.

Daraus ergeben sich zwei Fragen in Bezug auf den Entwurf des Cybersicherheitspakets:

1. Wird das Paket diesem transnationalen Charakter von Cyberoperationen gerecht? Denn obwohl die einzelnen Cyberoperationen unterhalb der Schwelle eines bewaffneten Konflikts liegen, entfalten sie in ihrer Gesamtheit disruptive Wirkung.
2. Ist das Subsidiaritätsprinzip Teil der Lösung oder verstärkt es das Problem, weil die mangelnde Transparenz über das Gesamtlagebild eher verstärkt wird?

Intensität und Umfang von Cybervorfällen im Jahr 2025

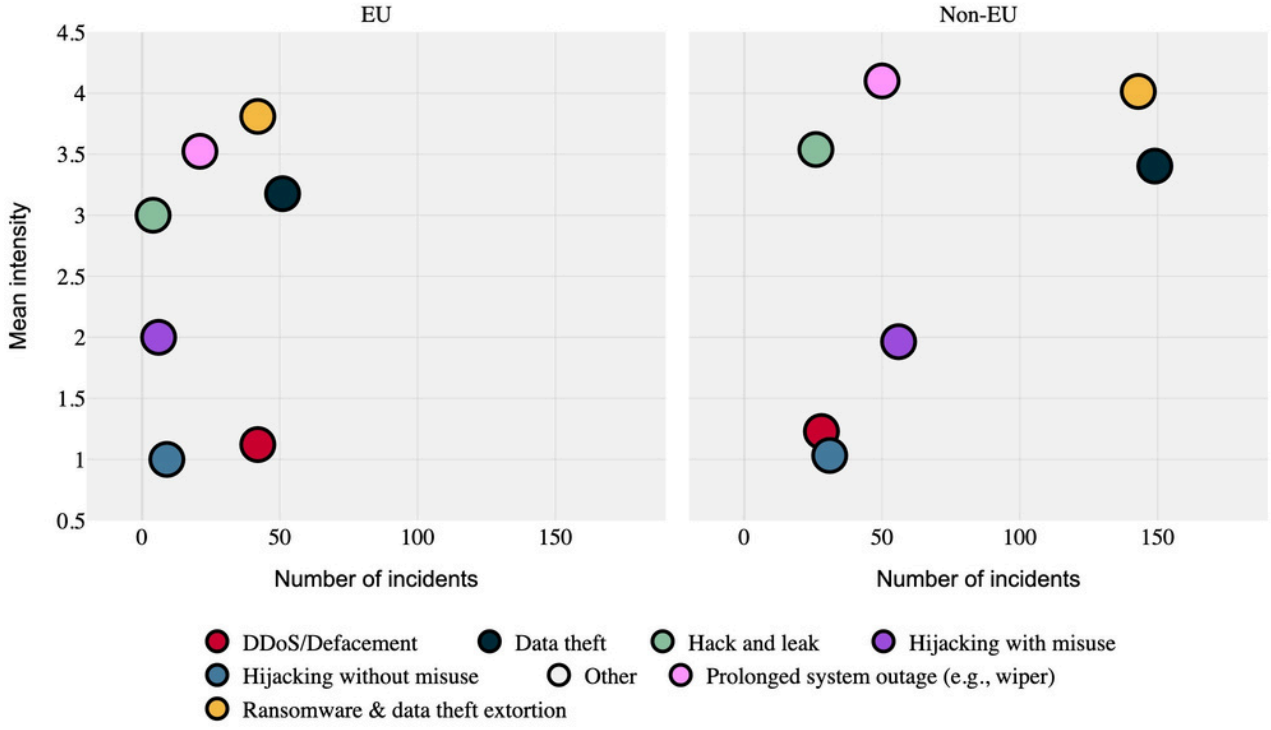
2025 war das erste Jahr seit Beginn der Pandemie, in dem EuRepoC weniger Cyberoperationen auf EU-Gebiet verzeichnet hat als im Vorjahr: Gegenüber dem Jahr 2024 ging die Zahl von 211 auf 179 zurück.

Parallel dazu stieg jedoch die Zahl der von diesen Operationen betroffenen EU-Ziele von 357 auf 388. Das ist ein Indiz dafür, dass einzelne Vorfälle zunehmend mehrere Organisationen gleichzeitig betreffen – eine Schlussfolgerung, die im Einklang mit der Zunahme von Angriffen auf Lieferketten und digitale Anbieter stehen würde.

Angesichts des leichten Rückgangs des weltweit (ohne EU-Mitgliedstaaten) erfassten Volumens der Operationen um 17,67 Prozent (von 583 auf 480) und eines Rückgangs der betroffenen Entitäten um 21,15 Prozent (von 1045 auf 824) deutet diese Entwicklung gleichzeitig auf eine Konzentration gegen Ziele in den EU-Mitgliedstaaten hin. Ein Rückgang war 2025 bei den durchschnittlichen Systemunterbrechungszeiten und dem Ausmaß des Datendiebstahls in der EU zu verzeichnen. Der Durchschnittswert des Intensitätsindikators sank entsprechend von 2,8 auf 2,6. Nur elf der Operationen erreichten die höchsten Intensitätsstufen fünf und sechs, im Vorjahr waren es 2024 noch 18 Operationen.

Weniger Intensität bedeutet allerdings nicht, dass die ausgelösten systemischen Störungen abgenommen hätten. So sind schwerwiegende kinetische Vorfälle in einzelnen Staaten wie in Norwegen als Nicht-EU-Mitglied nicht berücksichtigt. Auch der verhinderte schwere Angriff auf das polnische Stromnetz fließt nicht in die Statistik ein.

Intensität und Umfang von Cybervorfällen, die sich im Jahr 2025 gegen EU-Mitgliedstaaten und Drittländer richten



Quelle: EuRepoC Global Database, Stand: 03.02.2026.

Gerade russische staatliche Akteure haben ihren Fokus auf disruptive Aktionen verstärkt. Mehr als 69 Prozent der ihnen zugeschriebenen Operationen sind solche, im Vorjahr waren es noch 55 Prozent. Die Operationen verursachen weiterhin erhebliche Schäden im Energie- und Verkehrssektor.

Drei Intensiv-Ereignisse aus dem vergangenen Jahr sind besonders bemerkenswert:

1. **Norwegen** (April 2025): Russland-nahe Hacker übernahmen die Kontrolle über einen Wasserkraftdamm, öffneten Schleusen und ließen Wasser ab. Keine Opfer, aber der Beweis für kinetisches Schadenspotenzial.
2. **Frankreich** (Dezember 2025): Ein massiver DDoS-Angriff auf die französische Post störte Websites, Paketverfolgung und digitale Bankdienste während der Weihnachtszeit.
3. **Polen** (Dezember 2025): Ein koordinierter Angriff auf die nationale Energieinfrastruktur wurde erfolgreich abgewehrt, betraf aber erstmals mehrere Standorte gleichzeitig.

Trotz der Besonderheit, gibt es keine Anzeichen dafür, dass sie als „groß angelegte“ Vorfälle im Sinne von NIS-2 einzustufen sind. Sie richteten sich auch nicht gegen mehr als einen EU-Mitgliedstaat. Die entsprechenden Mitgliedstaaten waren in der Lage, die Störungen zu beheben. Dennoch sind die Angriffe Teil eines umfassenden Musters anhaltender Cyberaktivitäten gegen die EU.

Vier Beobachtungen zur Cyberbedrohungslage

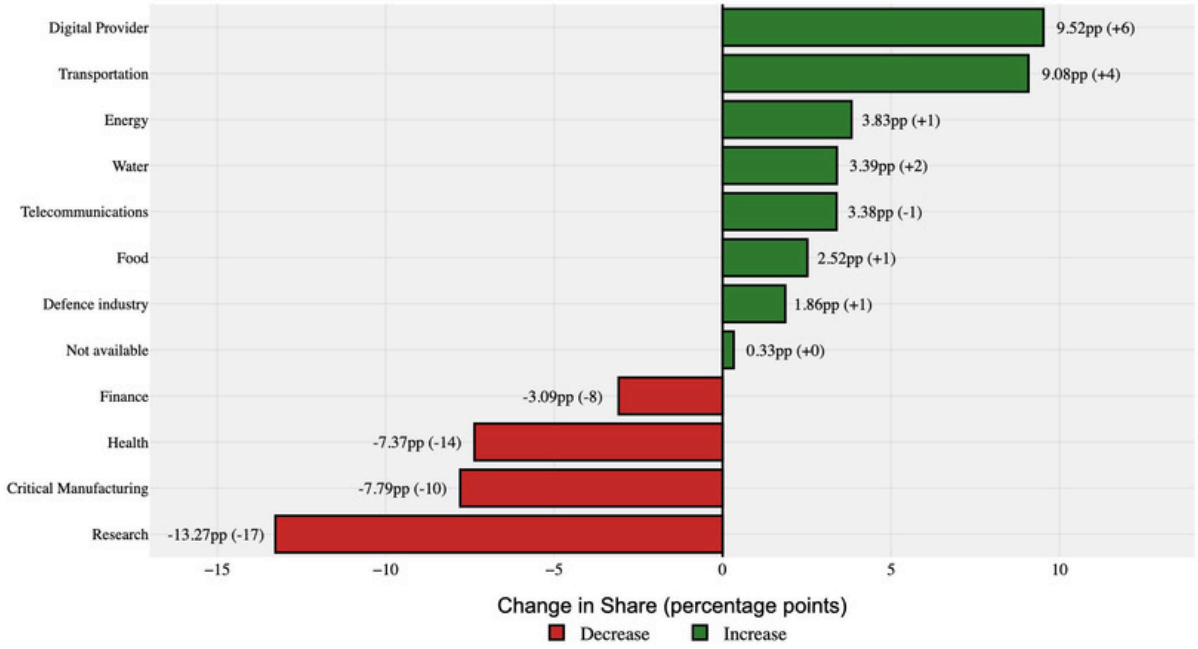
Vier Beobachtungen aus dem „2025 Balance” werfen daher die grundlegende Frage auf, ob die kumulative Wirkung von einzelnen schwerwiegenden Cyberangriffen die Anwendung der Solidaritätsklausel nach Art. 222 AEUV rechtfertigen kann.

Beobachtung 1: Die Art der Cyberbedrohungen, denen die EU-Mitgliedstaaten ausgesetzt sind, verschiebt sich.

Im Vergleich zu 2024 ist die Gesamtzahl der Cyberangriffe gegen Einrichtungen der kritischen Infrastruktur in den EU-Mitgliedstaaten tatsächlich von 115 auf 87 Vorfälle im Jahr 2025 zurückgegangen, jedoch hat sich die Verteilung der angegriffenen Sektoren im letzten Jahr erheblich verschoben. Anders als in den Vorjahren verzeichnete der Gesundheitssektor nicht mehr die meisten Vorfälle; mit 15 erfassten Angriffen liegt er nur noch auf Rang 2.

Stattdessen entwickelte sich der Verkehrssektor im Jahr 2025 zum meist betroffenen Sektor; sein Anteil an den Vorfällen stieg um 9,08 Prozentpunkte. Ein noch deutlicherer Anstieg war bei Angriffen auf digitale Anbieter zu beobachten, deren Anteil im Vergleich zum Vorjahr um 9,52 Prozentpunkte zunahm. Der Anstieg der Angriffe auf digitale Anbieter fällt mit der zunehmenden Konzentration der Angreifer auf die Ausnutzung digitaler Abhängigkeiten und Lieferketten zusammen. Die meisten Vorfälle bleiben unattribuiert oder werden kriminellen Gruppen ohne klares Herkunftsland zugeschrieben – Angriffe auf

Veränderung des Anteils an Cybervorfällen, die kritische Infrastruktursektoren der EU-Mitgliedstaaten betreffen (2024 auf 2025)



Quelle: EuRepoC Global Database, Stand: 03.02.2026.

digitale Anbieter ermöglichen jedoch schnelles Eindringen in zahlreiche vernetzte Organisationen mit massiven Datendiebstählen und weitreichenden Störungen.

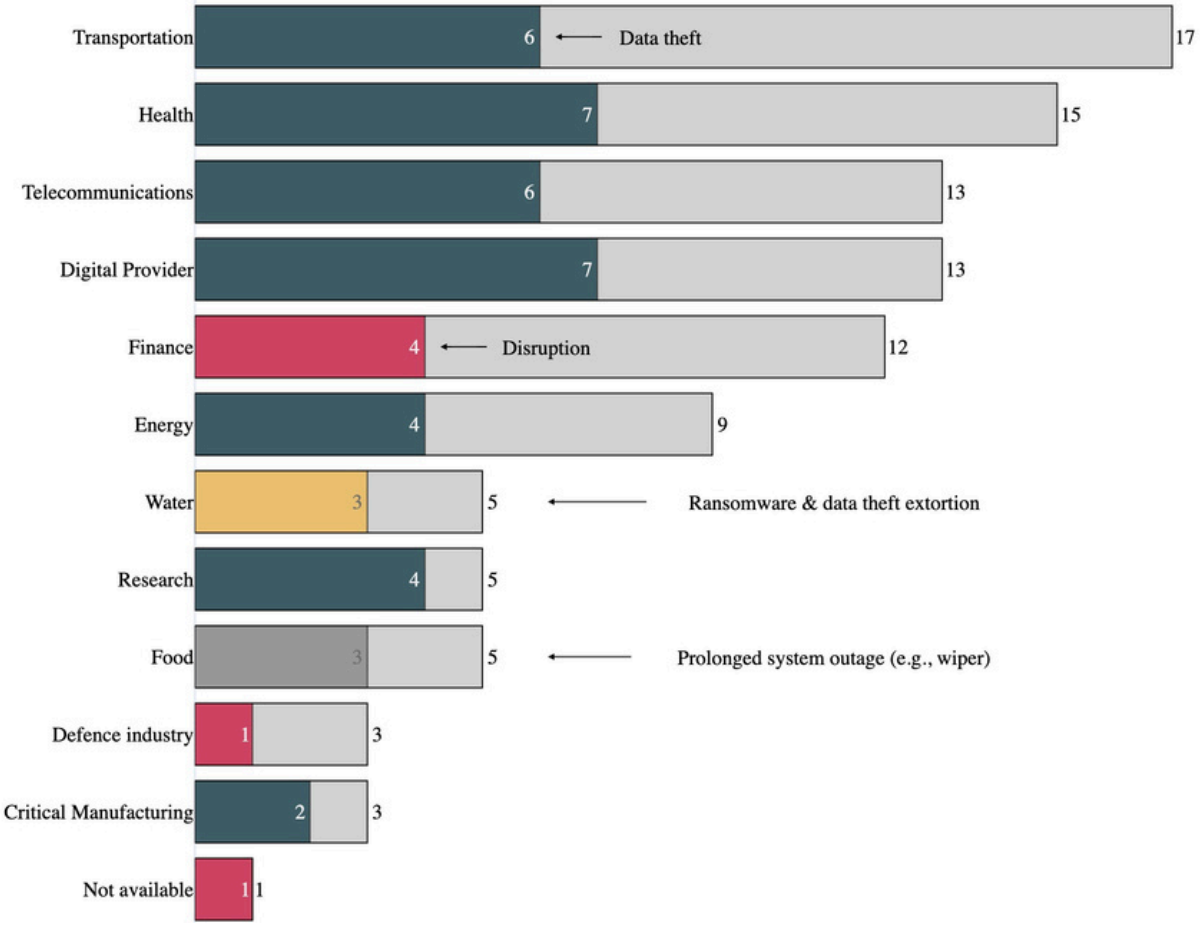
Ein Beispiel ist der Missbrauch der Anwendung Salesloft Drift: UNC6395 nutzte OAuthToken aus und drang in Dutzende Großunternehmen ein, darunter FedEx, Air France/KLM, Marriott und Cisco. Diese Unternehmen wurden anschließend von Scattered Lapsus$ Hunters erpresst.

Es gab zwei weitere besonders bemerkenswerte Angriffe in diesem Sektor: Den Angriff auf Collins Aerospace im September 2025, der zu einer weitreichenden Störung von mindestens sieben großen europäischen Flughäfen führte, sowie der Angriff auf den schwedischen IT-Dienstleister Miljödata im August, der zahlreiche Kommunen und Volvo North America betraf. Hier wurden später die Daten von 1,5 Millionen Schweden veröffentlicht. Ein großer Teil der übrigen Vorfälle, die sich gegen digitale Anbieter richteten, betraf speziell Unternehmen, die digitale Dienste für die Zivilverwaltung in Gemeinden in EU-Mitgliedstaaten erbringen. Die meisten davon waren bis Februar 2026 nicht attribuiert.

Verkehrssektor als Ziel russischer Gruppen

Von 18 Vorfällen im Verkehrssektor 2025 waren sieben disruptiv. Der Sektor ist erneut bevorzugtes Ziel der russischen Hacktivistengruppe NoName057(16). Obwohl nicht alle Angriffe öffentlich zugeordnet wurden, bekannte sich die Gruppe über Telegram zu einigen davon – etwa zu den Angriffen auf die deutschen Bahnbetreiber Hannover SBahn und

Am häufigsten betroffene kritische Infrastruktursektoren und Vorfallstypen in den EU-Mitgliedstaaten im Jahr 2025



Metronom. 2025 war auch das Jahr, in dem die deutsche Regierung den Angriff auf die deutsche Flugsicherung (DFS), der bereits im August 2024 stattfand, offiziell der vom russischen Staat unterstützten Gruppe APT28/Fancy Bear zuschrieb. Medienberichte hatten bereits kurz nach dem Angriff in 2024 auf eine russische Verantwortung hingewiesen.

Die übrigen Vorfälle im Transportsektor 2025 zeigten Muster von Datendiebstahl oder Ransomware. Der Anstieg im Sektor hängt auch mit Angriffen auf digitale Drittanbieter zusammen – so auch bei Cyberangriffen auf die Berliner Verkehrsbetriebe (BVG) und die Royal Mail.

Beobachtung 2: Ransomware ist eine grenzüberschreitende Bedrohung, die international bekämpft werden muss.

Ransomware- und andere kriminelle Gruppen sind nicht der Hauptgrund dafür, dass viele Cybervorfälle nicht eindeutig zugeordnet werden können. Im Gegenteil: Im Rahmen ihrer Erpressung bekennen sich diese Gruppen beispielsweise auf sogenannten Leak-Seiten meist selbst zu ihren Taten. Auch wenn das Repository diese Selbstaussagen nicht direkt überprüft, sondern sich auf öffentlich gemeldete Vorfälle und Zuschreibungen stützt, wurden 23 von 41 erfassten Ransomware-Angriffen (56 Prozent) in EU-Mitgliedstaaten öffentlich einer bestimmten Gruppe zugeordnet.

Auffällig ist dabei, dass bei diesen Zuschreibungen in der Regel kein Herkunftsland genannt wird. Das liegt zum einen daran, dass die Gruppen selbst kein Land angeben. Zum anderen agieren sie meist transnational: Sowohl die beteiligten Personen als auch ihre digitale Infrastruktur und ihre Zielauswahl sind international verteilt.

a) Transnationale Zielauswahl
Im Jahr 2025 griffen die zehn aktivsten kriminellen Gruppen mit Zielen in EUMitgliedstaaten ihre Opfer durchschnittlich in 3,9 Ländern weltweit an. Besonders aktiv war UNC6395, die in 11 Ländern tätig war. Es folgen die Everest-RansomwareGruppe mit Angriffen in 8 Ländern sowie Warlock, die Ziele in Europa, Nordamerika und Lateinamerika ins Visier nahm. Der Salesloft-Fall verdeutlicht, wie stark digitale Dienstleistungsplattformen international vernetzt sind: Wird ein solcher Anbieter angegriffen, können sich die Auswirkungen schnell über mehrere Länder hinweg ausbreiten.

Noch deutlicher wird die internationale Dimension, werden staatliche und staatlich unterstützte Akteure einbezogen. Dann steigt die Zahl der betroffenen Länder im Durchschnitt auf 12,2. Besonders hervorzuheben ist die nordkoreanische, staatlich unterstützte Gruppe Lazarus mit Aktivitäten in 31 Ländern. Auch chinesische Gruppen wie APT27 (Linen Typhoon) und APT31 (Violet Typhoon) waren jeweils in 13 Ländern aktiv.

Im Vergleich dazu zeigen sich russische Gruppen, die in EU-Mitgliedstaaten aktiv sind, anders ausgerichtet. Sie konzentrieren sich stärker auf gezielte Störangriffe und griffen im Durchschnitt nur 2,75 Länder an, mit einem klaren Fokus auf EUMitgliedsstaaten.

b) Transnationale Infrastrukturen und Einzelpersonen
Das Ökosystem der Cyberkriminellen-Netzwerke weist eindeutig transnationale Aspekte auf. Die „Criminal-as-a-Service"-Modelle (XaaS, d. h. Ransomware-as-a-Service) sind in vielen Ländern verbreitet und beschränken sich nicht nur auf Ransomware-Dienste. Während Russland Cyberkriminellen einen sicheren Hafen bietet, beschränken sich die Infrastrukturen und die Reichweite vieler Krimineller trotz einer Konzentration nicht unbedingt auf dieses Territorium.

Wie weitreichend und grenzüberschreitend diese Formen der Cyberkriminalität sind, wird häufig erst deutlich, wenn Staaten darauf reagieren. Ein Beispiel dafür ist der Juli 2025: Das US-Finanzministerium verhängte Sanktionen gegen die Aeza Group, einen in Russland ansässigen Anbieter sogenannter „Bulletproof-Hosting"-Dienst, weil das Unternehmen weltweit cyberkriminelle Aktivitäten unterstützte.

Die meisten Tochterfirmen von Aeza hatten ihren Sitz in Russland. Gleichzeitig nutzte die Gruppe mit Aeza International Ltd. eine Briefkastenfirma im Vereinigten Königreich. Über diese Firma wurden IP-Adressen an Cyberkriminelle vermietet, unter anderem an Betreiber der Schadsoftware Meduza Infostealer. Der Fall zeigt, wie kriminelle Infrastrukturen international organisiert sind und gezielt rechtliche und geografische Grenzen ausnutzen.

Die Ergebnisse der Operation Endgame bestätigen diese Beobachtung. Die koordinierte Operation, die erstmals 2022 gestartet wurde und an der Strafverfolgungsbehörden aus elf Staaten beteiligt waren, trat im November 2025 in die Phase drei ein. Die Aktion führte zur

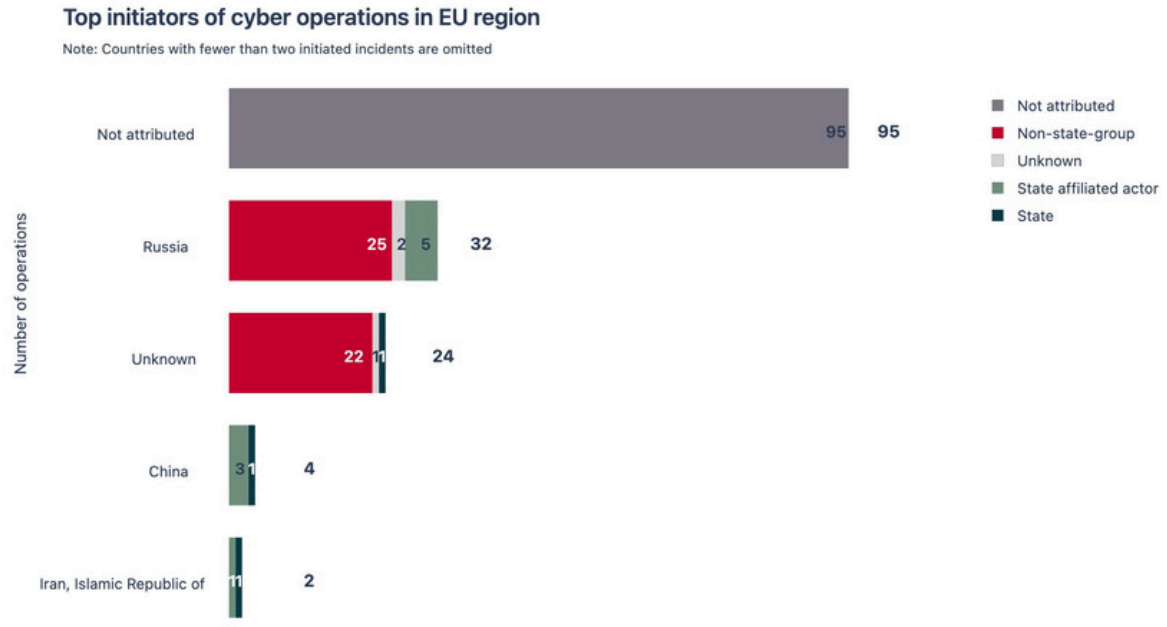
Durchsuchung von elf Standorten in Deutschland, Griechenland und den Niederlanden und zur Stilllegung von 1025 Servern weltweit. Ransomware-Gruppen agieren gleichzeitig aus verschiedenen Ländern heraus und greifen Ziele in mehreren Staaten an. Dabei nutzen sie ein immer größer werdendes Netzwerk krimineller Dienstleister, etwa für Schadsoftware, Hosting oder Geldwäsche. Auch die Erfolge der Strafverfolgungsbehörden sind inzwischen meist international koordiniert.

Das zeigt deutlich: Ransomware ist eine grenzüberschreitende Bedrohung und kann nur durch enge internationale Zusammenarbeit wirksam bekämpft werden.

Beobachtung 3: Eine wachsende Zahl von Proxy-Akteuren handelt im Namen oder mit Unterstützung von Staaten gegen die EU. So wird die Zuweisung staatlicher Verantwortung erschwert.

Im Jahr 2025 waren die EU-Mitgliedstaaten vor allem Ziel von Bedrohungsakteuren mit Verbindungen zu Russland und China. Ähnlich wie im Jahr 2024 konzentrierten russische Bedrohungsakteure sich vorrangig auf disruptive Cyberaktivitäten wie kostengünstige DDoS-Angriffe mit hoher Sichtbarkeit sowie langanhaltende Systemstörungen bei kritischen Infrastruktureinrichtungen.

Wichtigste Bedrohungsakteure von Cyberoperationen gegen EU-Mitgliedstaaten im Jahr 2025



Quelle: EuRepoC Global Database, Stand: 03.02.2026.

Trotz der offensichtlichen Dominanz russischer nichtstaatlicher Gruppen, insbesondere selbsternannter „Hacktivisten“, deuten die Entwicklungen im Jahr 2025 darauf hin, dass die Grenze zwischen staatlich gelenkten Operationen und vordergründig unabhängigen Hacktivisten-Kampagnen nicht weniger durchlässig ist als bei anderen Formen russischer Proxy-Aktivitäten.

Der aktivste Bedrohungsakteur in Europa war laut EuRepoC-Daten NoName057(16). Er ist seit März 2022 aktiv und wurde bis vor kurzem als pro-russische Hacktivisten-Gruppe angesehen. Die Gruppe ist bekannt für ihre groß angelegten DDoS-Kampagnen über ihre überwiegend von Freiwilligen betriebene Plattform „DDoSia“. Als Nachfolger des Bobik-Botnetzes umfasst DDoSia das gesamte Ökosystem an Tools, Infrastruktur und Freiwilligen, das für die Durchführung dieser langfristigen DDoS-Kampagne erforderlich ist. Eine weitere auffällige russische Gruppe, Z-Pentest, drang im April 2025 in das Wasserdamm-System in Norwegen ein und schaffte es, dessen Wasserventil stundenlang mit voller Kapazität zu öffnen, bevor der Cyberangriff entdeckt wurde.

Im Laufe des Jahres 2025 wurden neue Informationen über beide Gruppen veröffentlicht, die aufschlussreiche Details über deren Arbeitsweise enthielten. Die Erkenntnisse deuten auf eine direkte Verbindung der Gruppe NoName057(16) zum russischen Staat hin.

Bei Operation Eastwood im Juli 2025 gingen Europol und Behörden aus elf EU-Staaten sowie den USA gegen NoName057(16) vor. Es gab zwei Festnahmen und sieben Haftbefehle, die Infrastruktur wurde beschädigt. Die Gruppe tauchte jedoch am 23. Juli wieder auf und verstärkte ihre Angriffe auf kritische Infrastrukturen. Am 9. Dezember veröffentlichten die USA und Partner ein Joint Advisory, das die Hacktivistengruppe Carr mit der GRU-Einheit 74455 (Sandworm) verknüpfte. NoName057(16) wurde als Projekt des kremlnahen Zentrums CISM identifiziert, das Infrastruktur, Social Media und Zielauswahl steuert.

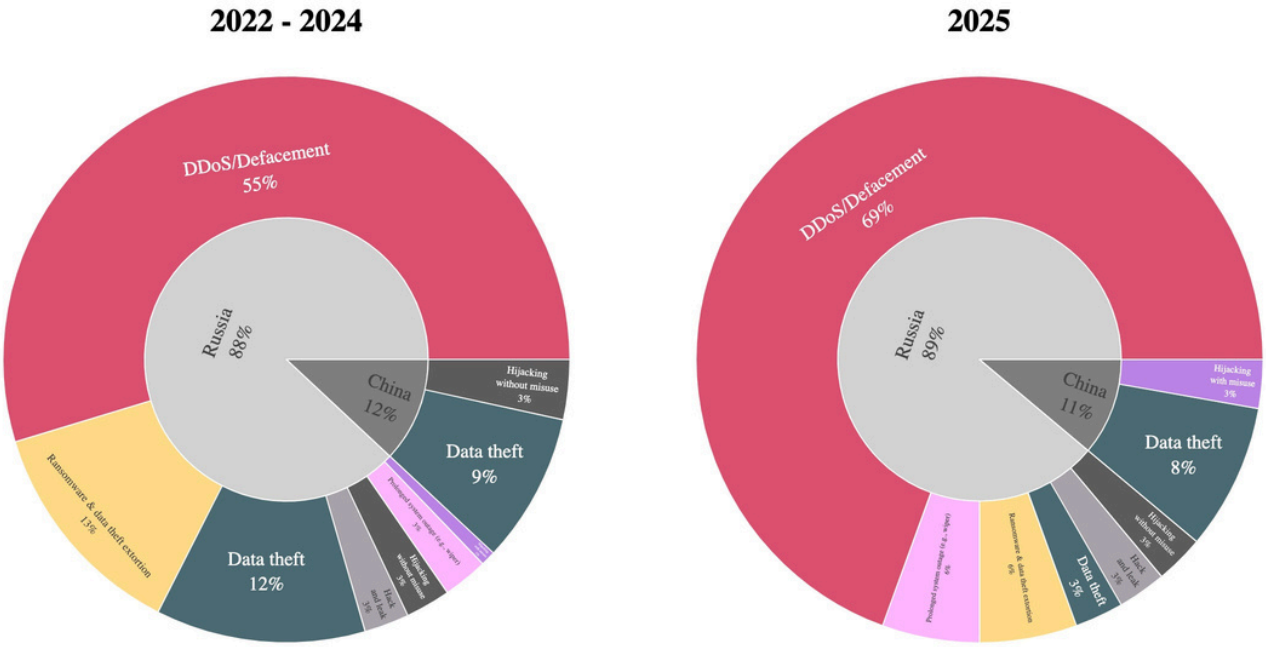
Russland bleibt ein Paradebeispiel dafür, wie die unklare Verbindung zwischen staatlichen und nicht-staatlichen Akteuren die Zuordnung erschwert. Während russische Akteure öffentlichkeitswirksam auftreten, agieren chinesische Akteure verdeckt.

Die geringe Zahl China zugeschriebener Vorfälle erklärt sich dadurch, dass die Berichterstattung meist auf Kampagnen statt Einzelfällen basiert. Chinesische Akteure nutzen oft bestimmte Schwachstellen aus und erreichen damit viele Organisationen weltweit, weshalb EuRepoC nur Zielsektoren statt spezifische Ziele erfassen kann.

Zudem konzentrieren sich chinesische Akteure auf Spionage und das Eindringen in Systeme, möglicherweise zur strategischen Vorbereitung künftiger Angriffe. Staatlich verbundene chinesische Akteure nutzen Ransomware offenbar auch als Ablenkung.

Dies zeigt der Missbrauch von CVEs vor deren Offenlegung durch APT27, APT31 und die 2025 aufgetauchte Warlock-Gruppe. Die tatsächliche Zahl chinesischer Aktivitäten ist daher wahrscheinlich verschleiert – allerdings zielten 2025 nur 4 von 34 zugeordneten chinesischen Operationen auf EU-Staaten.

Vorfälle russischer und chinesischer Herkunft gegen EU-Mitgliedstaaten



Quelle: EuRepoC Global Database, Stand: 03.02.2026.

Beobachtung 4: Es ist die Stärke der Gegner, die Schwächen der europäischen Koordinierung auszunutzen.

Trotz grenzüberschreitender Cyberbedrohungen gibt es kaum transparente multilaterale Koordinierung bei der Attribution spezifischer Vorfälle. EuRepoC definiert gemeinsame Attribution als Zuordnungserklärung, bei der mehrere Länder eine gemeinsame Bewertung vornehmen – im Gegensatz zu unabhängigen Einzelattributionen.

2025 verzeichnete das Repository keine einzige gemeinsame Attribution für Vorfälle gegen EU-Mitgliedstaaten. Bei Angriffen auf andere Staaten gab es dagegen fünf solcher Zuordnungen. In zwei Fällen waren neben den Five Eyes EU-Staaten beteiligt: einmal zur Verantwortung von APT28 für Angriffe auf Großbritannien, sowie einmal zum Einsatz chinesischer Spyware gegen uigurische, tibetische und taiwanesische Gruppen. Bezeichnend ist auch, dass Dänemark sich nicht am Joint Advisory vom 9. Dezember beteiligte und stattdessen neun Tage später unilateral attribuierte. Dies deutet auf eine Fragmentierung europäischer Ansätze und fehlende strukturierte Attributionsprozesse hin.

Das Werkzeug von Sanktionen wird weiterhin nur in wenigen Fällen genutzt. Was andere Reaktionen angeht, war Deutschland mit 17 nachverfolgten politischen Reaktionen im Jahr 2025 der aktivste EU-Mitgliedstaat, gefolgt von Frankreich (9), Italien (8) und Polen (6). Es gab jedoch nur einen einzigen Vorfall, der eine politische Reaktion von mehreren EUMitgliedstaaten auslöste: Als der Rat der EU zusammen mit der NATO und Tschechien am 28. Mai 2025 auf den

Hackerangriff auf ein Netzwerk des tschechischen Außenministeriums aus dem Jahr 2022 reagierte. Bemerkenswert ist, dass es keine spezifischen Solidaritätsbekundungen oder gemeinsamen Maßnahmen der europäischen Staaten zu den konkreten Vorfällen gab, die sich gegen den Risevatnet-Staudamm in Norwegen oder eine Wasseraufbereitungsanlage in Dänemark richteten. Stattdessen reagierten die betroffenen Staaten unilateral auf die jeweiligen Vorfälle.

Abgesehen von der oben erwähnten Solidaritätserklärung der EU zu den chinesischen Cyberangriffen auf das tschechische Außenministerium hat die EU lediglich eine zweite Erklärung abgegeben, in der sie die anhaltenden hybriden Kampagnen Russlands gegen die EU verurteilt. Darin unterstützte die EU mehrere frühere Attributionen von Mitgliedstaaten (zum Beispiel die deutsche und tschechische Attribution im Jahr 2024 und die französische Attribution im April 2025) sowie die neuen Sanktionen Großbritanniens als Reaktion auf die von der GRU geleiteten Cyberoperationen. Auch wenn die Erklärung der EU als Versuch verstanden werden kann, eine geeinte europäische Front zu präsentieren, dominieren in der Praxis doch eher fragmentierte Ansätze statt strategischer Zusammenarbeit.

Fazit: Ist Solidarität eine subsidiäre Aufgabe?

Das künftige Mandat der ENISA ist laut Entwurf eng an die Koordinierungsmechanismen des Cyber Solidarity Act (CSA) gebunden, die vor allem bei „groß angelegten Cybervorfällen" im Sinne der NIS2-Richtlinie aktiviert werden.

Die empirischen Daten zeichnen jedoch ein komplexeres Bild: Bedrohungen treten heute oft nicht als einzelne spektakuläre Angriffe auf, sondern als anhaltende, strategisch abgestimmte Kampagnen – insbesondere, wenn mutmaßlichen Verbindungen zu Russland bestehen. Damit stellt sich die Frage, ob die derzeitigen Schwellenwerte noch angemessen sind. So mögen russische Cyberoperationen selten die Kriterien eines „groß angelegten" Angriffs erfüllen, in ihrer Gesamtheit können sie die Widerstandsfähigkeit jedoch erheblich schwächen.

Vor diesem Hintergrund sollte auch die Solidaritätsklausel nach Artikel 222 AEUV in den Blick genommen werden: Wenn koordinierte Cyberoperationen systemische Auswirkungen haben, kann ihre Gesamtwirkung solidarisches Handeln rechtfertigen – selbst ohne formale Schwellenwertüberschreitung. Eine flexiblere Auslegung, die strategische Gesamtwirkungen berücksichtigt, erscheint notwendig.

Die Frage, ob die kumulative Dynamik des heutigen Cyberkonflikts ausreichend erfasst wird, stellt sich auch angesichts der zurückhaltenden europäischen Zusammenarbeit bei der öffentlichen Zuschreibung von Cyberangriffen. Auch hier liegt es nahe, die bislang bestehenden Koordinierungs- und Solidaritätsmechanismen der EU zu überprüfen. Auch hier könnte eine flexiblere Auslegung nötig sein, um die strategische Gesamtentwicklung adäquat widerspiegeln zu können.

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 geleitet von der Universität Heidelberg, in Kooperation mit der Universität Innsbruck, der Stiftung Wissenschaft und Politik und dem Cyber Policy Institute (Estland). Es wird aktuell durch das Auswärtige Amt und die Allianz gefördert.

Der Beitrag ist im Rahmen des Projekts "Europäische Diplomatie und Normbildung. Potentiale für die Cyber-Incident- und Responseforschung heben" entstanden, finanziert durch den Cyberaußenpolitikstab des Auswärtige Amts.

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

European
Repository of
Cyber Incidents

www.eurepoc.eu

UNIVERSITÄT HEIDELBERG ZUKUNFT SEIT 1386

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

universität innsbruck

CPI CYBER POLICY INSTITUTE