European
Repository of
Cyber Incidents

EuRepoC
Cyberkonflikt Briefing

Q1 2026

Kerstin Zettl-Schabath
Jonas Hemmelskamp
Lena Rottinger
Erik Kellenter

Beobachtungen zur Gesamtlage

Im ersten Quartal 2026 (Q1) wurden **187 Cyberoperationen** in die Datenbank aufgenommen. Obwohl das einen Rückgang um 10 Prozent gegenüber dem Vorquartal entspricht, richtet sich das Volumen damit wieder am langfristigen Quartalsdurchschnitt aus, nachdem 2025 ein Höhepunkt an Aktivität erreicht worden war.

Mit **45 Operationen entfällt fast ein Viertel aller erfassten Vorfälle auf die Vereinigten Staaten**. Damit sind sie weiterhin der mit Abstand am häufigsten betroffene Staat. Trotz des Beginns der Militäroperation gegen den Iran am 28. Februar gibt es hinsichtlich der gegen die USA gerichteten Operationen bislang keine messbare Abweichung vom langfristigen Quartalsdurchschnitt.

Im Aggregat übertrifft die Zahl der auf EU-Mitgliedstaaten verübten Angriffe erneut das Niveau in den Vereinigten Staaten. Mit 57 Operationen waren die 27 Staaten von einem Drittel aller Cyberoperationen betroffen. Auch EU-Institutionen waren betroffen, ein eher seltener Fall.

Über das Briefing

Das *Cyber Conflict Briefing* analysiert Entwicklungen in der Bedrohungslandschaft auf Grundlage der von **EuRepoC** erfassten Cybervorfällen. Für diese Auswertung stehen technische, politische sowie rechtliche Aspekte im Vordergrund. Seit Oktober 2025 veröffentlicht EuRepoC das Briefing quartalsweise in Zusammenarbeit mit der **Deutschen Cyber-Sicherheitsorganisation GmbH (DCSO).**

Die deutsche Ausgabe erscheint in Kooperation mit dem **Tagesspiegel Cybersecurity Background.**

Über EuRepoC

Das European Repository of Cyber Incidents ist ein europäisches Forschungsprojekt mit dem Ziel, Informationen und Wissen über Cyber-Konflikte 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 das dänische Außenministerium gefördert.

Weitere Informationen finden Sie unter https://eurepoc.eu

Geografische Verteilung von Cyberoperationen im 1. Quartal 2026

Zum einen wurde am 30. Januar bekannt, dass die zentrale Infrastruktur der Europäischen Kommission zur Verwaltung mobiler Endgeräte von einem Cyberangriff betroffen war; möglicherweise wurden Namen und Mobilfunknummern einiger Mitarbeiterinnen und Mitarbeiter geleakt. Zum anderen entwendete die Ransomware-Gruppe ShinyHunters bei einem Supply-Chain-Angriff am 24. März mindestens 340 GB aus der Cloud der Europäischen Kommission.

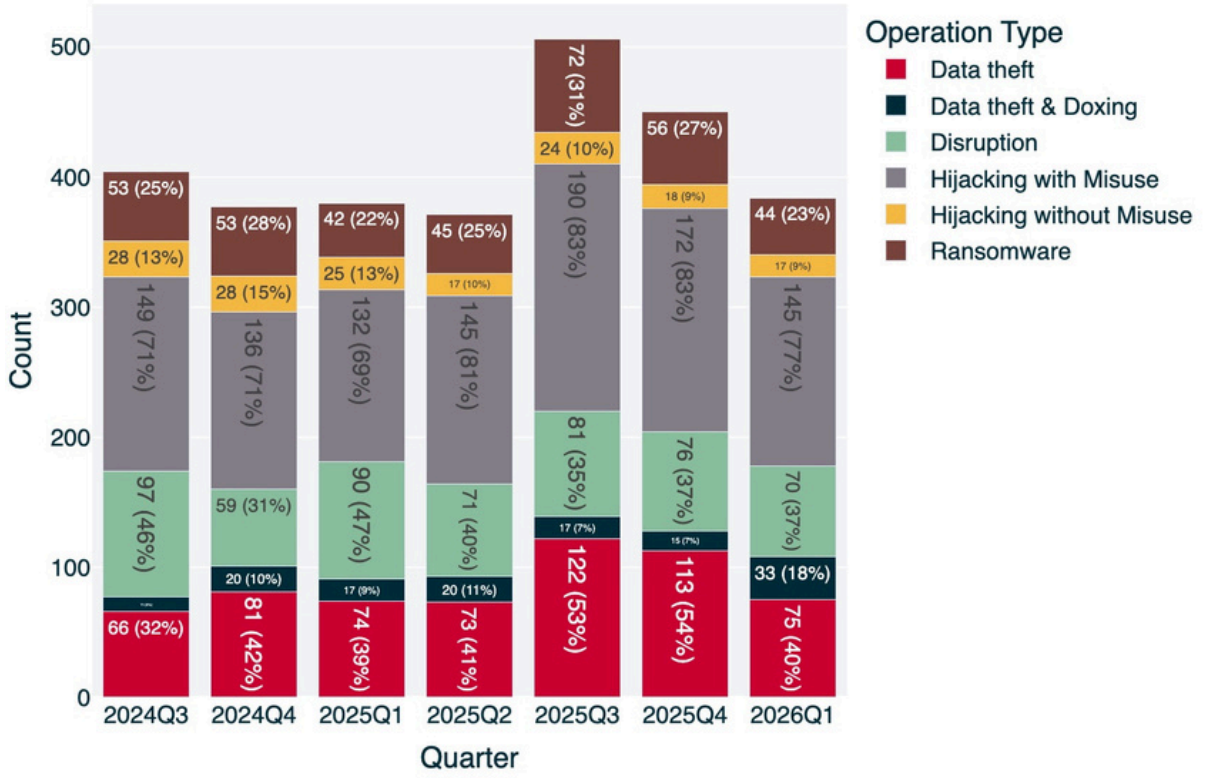
Auf nationaler Ebene war Frankreich mit 14 Vorfällen erneut der am zweithäufigsten betroffene Staat. Unbekannte Hacker drangen in die nationale Bankkontendatenbank FICOBA ein und griffen auf Daten von 1,2 Millionen Bankkonten zu. Ein weiterer Vorfall betraf die HR-Software des Ministeriums für nationale Bildung. Es wurden personenbezogene Daten von Mitarbeitenden des nationalen Bildungswesens geleakt. Auf Frankreich folgen Deutschland und Spanien mit jeweils 10 Vorfällen. In Q1 wurde die erste Cyberoperation in Grönland beobachtet, bei der ein lokales Busunternehmen Opfer eines DDoS-Angriffs wurde.

Brennpunkte und Zielmuster

Die relative Verteilung der Operationstypen ist gegenüber dem Vorquartal konstant geblieben. Der größte Anteil von 144 Vorfällen (77 %) entfällt auf die Kategorie „Hijacking with Misuse". Diese Kategorie wird in der Regel zusammen mit weiteren Typen wie „Data Theft" oder „Disruption" kodiert. Im März gaben beispielsweise mehrere Sicherheitsunternehmen, darunter Google, bekannt, dass eine Gruppe mit Verbindungen zum russischen Staat im Jahr 2025 zwei hochentwickelte iOS-Exploit-Toolkits, Coruna und DarkSword, übernommen hat, die ursprünglich von kommerziellen Überwachungsanbietern entwickelt worden waren. Diese Werkzeuge wurden gegen die ukrainische kritische Infrastruktur und den Militärsektor eingesetzt, wobei mehrere Zero-Day-Schwachstellen und neuartige Exploit-Techniken genutzt wurden.

„Data Theft" stellt den zweithäufigsten Operationstyp dar und macht 76 Vorfälle (41 %) aus. Eine gesonderte Kategorie, „Data theft & doxing", erfasst alle Operationen, bei denen Angreifer die exfiltrierten Daten anschließend veröffentlichen. Der relative Anteil dieser Vorfälle mit Veröffentlichung von Daten hat sich im Vergleich zum

Verteilung der Arten von Cyberoperationen



Vorquartal von 7 % auf 17 % mehr als verdoppelt. Diese Beobachtung dürfte mit der Zunahme von Cyberoperationen iranischer Akteure gegen Ziele vorrangig in Israel und den Vereinigten Staaten zusammenhängen. Das Leaken von Daten dient in diesem Rahmen neben zerstörerischen „Wiper"-Operationen als ein Mittel der öffentlichen Demonstration von Cyberfähigkeiten.

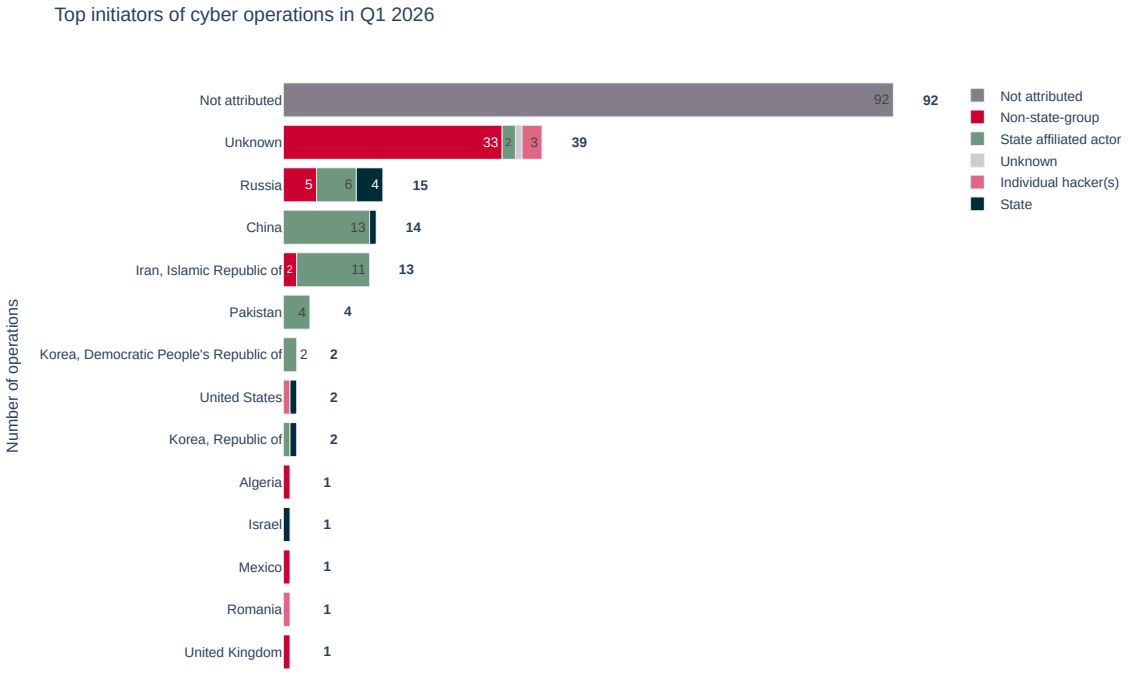
Gegen Ende März kompromittierte etwa die iranische Gruppierung Handala, das Gmail-Konto von FBI-Direktor Kash Patel und veröffentlichte persönliche Daten, die angeblich aus der Kompromittierung des Gmail-Kontos stammen sollen. Das FBI erklärte dagegen, dass keine sensiblen Regierungsinformationen entwendet worden seien.

Der Anteil der Vorfälle mit Disruption ist mit 37 % so hoch wie im Vorquartal. Der Anteil der DDoS-Angriffe in dieser Kategorie ging jedoch trotz des Irankonflikts von 20% auf 10% zurück. In den letzten drei Jahren war die russisch verbundene Gruppe NoName057(16) für einen großen Anteil aller erfassten DDoS-Angriffe verantwortlich, doch nach einem Höhepunkt im Jahr 2025 ging die Zahl der auf diese Gruppe zurückführbaren Operationen drastisch zurück. Im letzten Quartal wurde daraufhin lediglich ein DDoS-Angriff während der Olympischen Winterspiele in Italien erfasst.

Angreiferprofile und Attributionen

In Q1 gingen die meisten Cyberoperationen von russischen, chinesischen und iranischen Bedrohungsakteuren aus. Wie in den vorherigen Quartalen wiederholen sich gewisse Angriffsmuster: Russische Akteure fokussierten sich tendenziell eher auf destruktive und disruptive Angriffe, chinesische Akteure extrahierten hauptsächlich Daten und spionierten. EuRepoc dokumentierte zudem einen deutlichen Anstieg von Cyberaktivitäten, die auf Hackergruppen der iranischen Regierung zurückzuführen sind.

Verteilung der Arten von Cyberoperationen



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

Im Januar 2026 stand primär eine russische Cyberoperation auf polnische Energieinfrastrukturbetreiber im Fokus der Berichterstattung, für die gleich mehrere sich teilweise widersprechende Attributionen vorliegen. Der polnische Premierminister Donald Tusk bezeichnete die Angreifer in einer offiziellen Pressemitteilung als “Gruppierungen, die direkte Verbindungen zu russischen Nachrichtendiensten aufwiesen.” Welche Gruppierungen genau für den Angriff verantwortlich waren, sagte er nicht. Kurz darauf gab das polnische CERT (CERT.PL) an, dass die Infrastruktur der Angreifer sehr große Ähnlichkeit mit dem russischen Bedrohungsakteur “Static Tundra” (aka Bersek Bear, Ghost Blizzard, Dragonfly) aufweise. Diese Gruppe wurde bereits von US-Behörden dem russischen Inlandsgeheimdienst FSB zugeordnet.

Abweichend davon attribuierten die IT-Sicherheitsunternehmen ESET und Dragos den russischen Bedrohungsakteur “Sandworm”. Dieser war bereits für erfolgreiche Angriffe auf ukrainische Energiebetreiber in den Jahren 2015 und 2016 verantwortlich und verfügt über ein tiefes Verständnis elektrischer Infrastrukturen. Während Sandworm lange vor allem in der Ukraine aktiv war, deuten Berichte seit Ende 2025 auf Einsätze auch in Europa und Nordamerika hin. Die polnische Regierung hat Sandworm bislang nicht offiziell verantwortlich gemacht; auch das polnische CERT sieht keine eindeutigen Belege für eine Beteiligung in diesem Fall.

In einem Punkt waren sich jedoch alle Attributionen einig: Die Absicht der Angreifer war eindeutig destruktiv. Wenn der Angriff gelungen wäre und es tatsächlich zu einem großen Netzausfall gekommen wäre, so hätte das im tiefsten polnischen Winter vermutlich verheerende Auswirkungen gehabt.

Neben russischen Bedrohungsakteuren standen im ersten Quartal 2026 insbesondere iranische Akteure im Fokus der Berichterstattung. Seit Beginn des Irankonflikts am 28. Februar verzeichnete EuRepoC einen deutlichen Anstieg bösartiger Aktivitäten, die direkt oder indirekt mit der iranischen Regierung in Verbindung stehen. Die Angriffe richteten sich vor allem gegen kritische Infrastruktur und staatliche Einrichtungen in den USA, Israel und den Golfstaaten. Europa blieb bislang weitgehend verschont, mit Ausnahme von Irland (Standort von Stryker) und Albanien.

Für etwa die Hälfte der iranischen Vorfälle bekannte sich die vermeintlich hacktivistische Gruppierung “Handala”. Handala kompromittierte unter anderem den medizintechnischen US-Großkonzern Stryker. Das FBI stufte daraufhin Handala als Akteur ein, der im Auftrag des iranischen Ministeriums für Nachrichtenwesen (MOIS) handelt. Zudem stellte das FBI eine Verbindung zwischen Handala und einer weiteren iranischen Persona namens “Homeland Justice” her, die in den vergangenen Jahren hauptsächlich Albanien im Visier hatte.

Vor einem möglichen Anstieg von iranischer Hackeraktivitäten warnten zu Konfliktbeginn bereits mehrere Staaten, darunter das Vereinigte Königreich und Kanada. Auch die USA reagieren verstärkt auf die Cyberbedrohungen der iranischen Regierung, indem nicht nur mehrere Domains der Handala-Gruppierung beschlagnahmt wurden, sondern auch eine Belohnung in Höhe von 10 Millionen US-Dollar für Informationen über Hacker, die für die iranische Regierung arbeiten, verkündet wurde. Zudem veröffentlichten US-Behörden gleich mehrere technische Advisories, die darauf hindeuten, dass insbesondere kritische Infrastrukturen in den USA im Visier iranischer Hacker sind. Eine Analyse der iranischen Angriffe zeigt ein eindeutiges Muster: Staatlich-unterstützte iranische Bedrohungsakteure haben eine neue Präferenz für öffentlichkeitswirksamere, destruktive und disruptive Operationen. Das steht im Kontrast zu früherer iranischer Cyberaktivität, die in den vergangenen 25 Jahren eher auf Spionage und Aufklärung abzielte. Dafür, dass der Iran ein umfassendes System von staatlichen und staatlich unterstützten Hackergruppen unterhält, erwiesen sich die tatsächlichen Fähigkeiten im Cyberraum im Konfliktverlauf als vergleichsweise begrenzt.

Der Konflikt zeigte auch, wie Israel und die USA Cyberoperationen nutzen, um kinetische Operationen zu ergänzen oder zu verstärken. Dies geschieht zum Teil durch Beeinflussungskampagnen oder durch die Nutzung von Mobilgeräten und Überwachungskameras für die Zielauswahl und Schadenserfassung.

Entwicklungen im Bereich der Cyberkriminalität

Zentrale Beobachtungen aus Q1 lassen sich wie folgt zusammenfassen:

- Das Open-Source-Ökosystem entwickelte sich in Q1 weiter zu einem zentralen Einfallstor für kriminelle und staatlich-affiliierte Akteure. Kompromittierte npm-Pakete wie von Axios auf GitHub zeigen, wie Supply-Chain-Angriffe Tausende von Nutzern erreichen können. Die komplexen Abläufe vom initialen Zugriff bis hin zu Downstream-Angriffen erhöhen zudem das Risiko eines nachhaltigen Vertrauensverlusts in das Ökosystem. Nicht nur einzelne Pakete werden infiziert, sondern auch die auf Vertrauen

basierende Build-/Release-Pipeline wird zum Verteilungsvektor umfunktioniert. Bemerkenswert ist zudem die berichtete Kooperation zwischen der in Q1 hierfür zentralen Cybercrime-Gruppe Team PCP und dem jüngeren RaaS-Kollektiv Vect, um das gesamte Monetarisierungspotenzial auszuschöpfen.

- Das Bekanntwerden von gleich zwei Phone-Exploit-Kits, Coruna und DarkSword, die monatelang nicht nur von staatlichen Gruppen aus Russland, sondern auch von chinesischen Crypto-Kriminellen als Zero-Days ausgenutzt wurden, deutet auf eine zunehmende Proliferation von Zero-Days als „Second-Hand"-Ware hin, mutmaßlich verkauft durch zentrale Broker an unterschiedliche Endkunden.
- Der Konflikt zwischen den USA, Israel und dem Iran zeigte weitere Verbindungen zwischen kriminellen und staatlich-affiliierten Akteuren, etwa zwischen Handala (aka Void Manticore) und dem Radamanthys-Infostealer. Ferner agieren nordkoreanische APTs als Affiliates krimineller „as-a-service"-Modelle – hier der Medusa-Gang. So entstehen für Kriminelle neue Geschäftsfelder, während staatliche Akteure Kosten für den initialen Zugriff sparen.
- Weitere Erkenntnisse ermöglichten die Angreifer durch OPSEC-Fehler selbst: Ein nordkoreanischer Akteur infizierte sich mit dem LummaC2-Infostealer, wodurch seine Beteiligung am Polyfill.io-Supply-Chain-Angriff nachgewiesen werden konnte. In einem weiteren Fall begünstigte die INC-Ransomware-Gruppe durch die wiederholte Nutzung derselben Backup-Infrastruktur die Sicherstellung gestohlener Daten von 12 Organisationen.
- Auch in Q1 etablierte sich die ClickFix-Technik als mittlerweile omnipräsente Social-Engineering-Technik, mit weiterhin aufkommenden Unterformen, etwa der sog. „CrashFix"-Variante der Gruppe KongTuke. Diese bringt den Browser des Opfers absichtlich zum Absturz und veranlasst, schädliche Befehle sowie einen bislang nicht dokumentierten Python-RAT auszuführen.
- KI gewinnt auch im Ransomware-Umfeld weiter an Bedeutung: Laut IBM nutzte die Gruppe Hive0163 ein KI-generiertes C2-Framework, das einfacher umzusetzen und risikoärmer ist als etwa autonome KI-Agenten. Jedoch war das Fazit, dass auch hier der Einsatz von KI primär der Beschleunigung der Angriffsphasen diente und weniger eine neuartige Bedrohungsform an sich darstellte.
- In einem anderen Fall umfangreichen Datendiebstahls aus Mexiko, der neun Regierungsbehörden betraf, verwendeten die Angreifer Anthropic's Claude Code und OpenAI's GPT-4.1, ebenfalls für die drastische Verkürzung der Angriffszeitspanne, sowie um Rohdaten aus der Aufklärung von Hunderten Servern in strukturierte und nutzbare Informationen zu transformieren.
- Wie bereits 2025 fokussierten sich Affiliates besonders aktiver RaaS-Gruppen (z.B. Qilin und SafePay) auch in Q1 2026 verstärkt auf kleine und mittlere Unternehmen aus Deutschland, gerade im Bereich Fertigung/Herstellung. Auch hier spielt KI eine Rolle, um die Sprachbarriere zunehmend zu überbrücken.

- Auf technischer Ebene integrieren Ransomware-Akteure zudem zunehmend EDR-Killer in ihre Operationen, um Sicherheitsmechanismen kurz vor der Verschlüsselung von Daten auszuschalten. Hierbei setzen die Kriminellen zunehmend auf die „Bring your own vulnerable driver“-Technik, um ihre Zugriffsprivilegien auf die notwendige Systemebene (Kernel-Mode) auszuweiten.
- Aber auch die Strafverfolgungsseite und deren Partner blieben in Q1 sehr aktiv: Es erfolgten mehrere Takedowns, etwa des russischsprachigen Underground-Forums RAMP durch das FBI sowie die zumindest zeitweilige Abschaltung der Infrastruktur des Phishing-as-a-Service-Anbieters Tycoon2FA, der jedoch seine Aktivitäten nach kurzer Zeit wieder aufnahm. Zudem unternahm Google gemeinsam mit anderen Partnern eine Aktion gegen das weltweit größte Residential-Proxy-Network IPIDEA, mit dessen Diensten Cyberkriminelle und staatliche APTs ihre Identität verschleiern können.

Mehr von EuRepoC

EuRepoC informiert mit einem täglich kuratierten Cyber Incident Tracker über neu in die Datenbank aufgenommene Cybervorfälle. Diesen können Sie hier abonnieren.

About the authors

Kerstin Zettl-Schabath ist Senior Cyber Threat Intelligence Analyst bei dem Deutschen Cyber-Sicherheitsorganisation (DCSO).

Jonas Hemmelskamp ist Chef-Datenanalyst ("Chief Data Scientist") für das EuRepoC-Projekt und Doktorand an der Universität Heidelberg.

Lena Rottinger ist Masterabsolventin der Universität Heidelberg und ist wissenschaftliche Mitarbeiterin im EuRepoC-Projekt; sie ist verantwortlich für die politische Kodierung von Cybervorfällen.

Erik Kellenter ist Studentischer Mitarbeiter bei der Stiftung Wissenschaft und Politik (Berlin) und studiert seinen Bachelor in Politikwissenschaft und Master in Computerwissenschaft.

Follow us on social media

@EuRepoC

linkedin/EuRepoC

contact@eurepoc.eu

https://eurepoc.eu