European
Repository of
Cyber Incidents

EuRepoC Cyber Conflict Briefing

2023 CYBER ACTIVITY BALANCE

Jakob Bund
Kerstin Zettl-Schabath
Martin Müller
Camille Borrett

INHALTSÜBERSICHT

Über das Briefing

Analysen für das Cyber Conflict Briefing werden von EuRepoC erstellt. Die deutsche Ausgabe wird in Zusammenarbeit mit dem **Tagesspiegel Cybersecurity Background** veröffentlicht.

Das Briefing fasst die zentralen Trends, Dynamiken und Befunde zu den von EuRepoC in einem bestimmten Monat erfassten Cybervorfällen zusammen. Diese müssen nicht unbedingt in diesem Monat stattgefunden haben, sondern können auch früher begonnen haben. Dabei stehen technische, politische sowie rechtliche Aspekte im Vordergrund.

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.

Nähere Informationen zum EuRepoC-Projekt finden Sie hier.

1 Allgemeine Beobachtungen

1.1. Anzahl der erfassten Cyberoperationen:

895

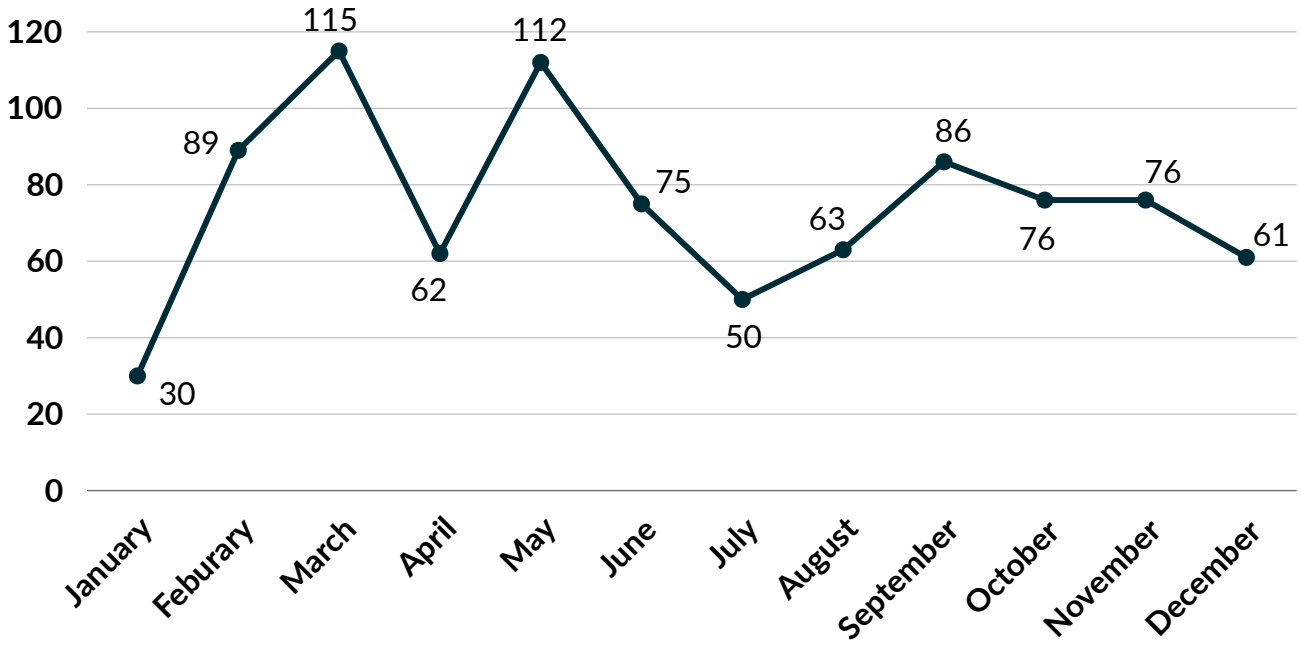
neue Cyber-Operationen im Jahr 2023

75

Operationen im Durchschnitt pro Monat

Im Jahr 2023 verzeichnete das European Repository of Cyber Incidents (EuRepoC) insgesamt **895 neue Cyber-Operationen**, was einem Durchschnitt von etwa 75 Operationen pro Monat entspricht. Im März und Mai wurden mit 115 bzw. 112 neuen berichteten Vorgängen bemerkenswerte Aktivitätsspitzen verzeichnet. In den Sommermonaten war dagegen ein Rückgang der gemeldeten Operationen zu verzeichnen.

Anzahl der erfassten Cyberoperationen pro Monat im Jahr 2023:

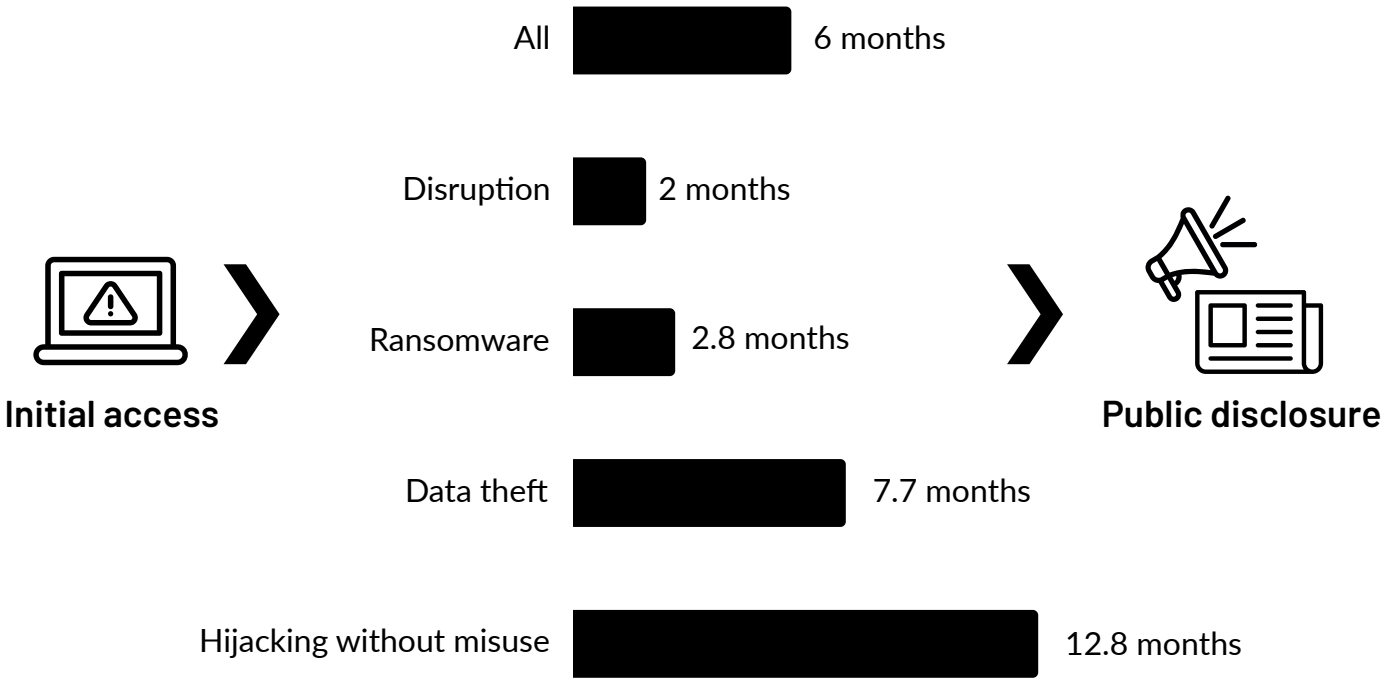


1.2. Zeitliche Verzögerung zwischen erstmaligem Angriff und öffentlicher Berichterstattung

Wir erfassen Daten zu Cyber-Operationen aus verschiedenen Quellen, einschließlich Blogs der IT-Community, Regierungsberichten und Medienartikeln, sobald sie veröffentlicht werden. Der aufgezeichnete Monat einer Operation stimmt daher nicht unbedingt mit ihrem tatsächlichen Startdatum überein.

Im Durchschnitt begannen die im Jahr 2023 erfassten Cyberoperationen **etwa sechs Monate vor dem Zeitpunkt, an dem sie öffentlich bekannt wurden**. Die Dauer der Offenlegung hängt von der Art der Cyberoperation ab. Vorgänge, bei denen es um Störungen und/oder Ransomware ging, werden im Allgemeinen schneller publik gemacht, in der Regel innerhalb von 2 bis 2,8 Monaten, da sie sichtbare und störende Auswirkungen haben und bestimmte Bedrohungsakteure Anreize haben, diese öffentlich - auch in überhöhter Art und Weise - an öffentlich bekannt zu machen. Vorgänge, die durch Datendiebstahl und/oder Hijacking ohne Missbrauch gekennzeichnet waren, wurden dagegen oft viel später gemeldet, im Durchschnitt 7,7 bzw. 12,8 Monate nach dem erstmaligen Zugriff.

Verzögerung in Monaten zwischen dem ersten Zugriff und der öffentlichen Bekanntgabe der im Jahr 2023 erfassten Cyber-Operation:

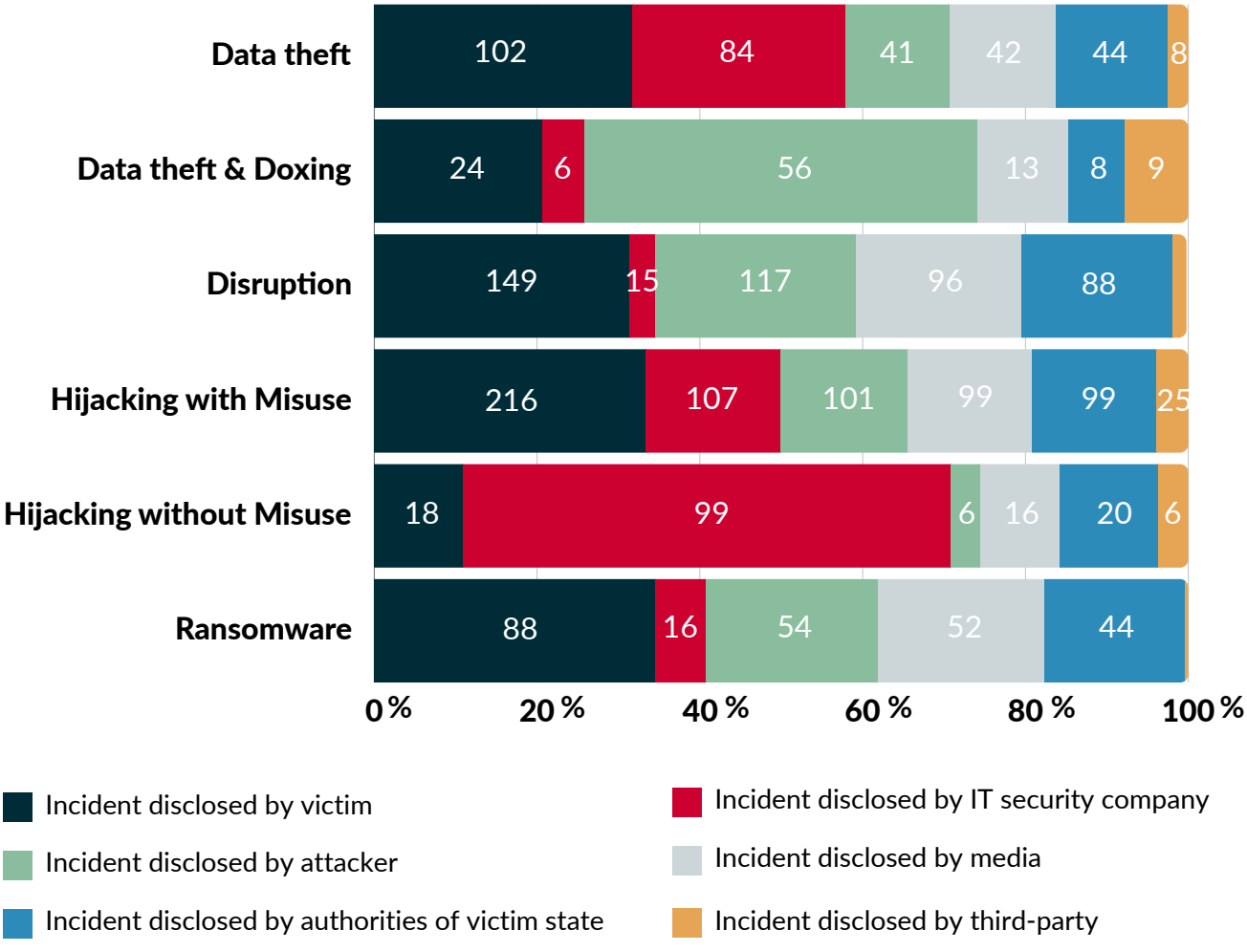


1.3. Wer veröffentlicht Cybervorfälle?

Der größte Anteil der im Jahr 2023 erfassten Cyberoperationen wurde von den **Opfern des Vorfalls** gemeldet (29 %, insgesamt 264), gefolgt von **IT-Sicherheitsunternehmen** (24 %, insgesamt 212). In 21 % der Fälle (189 insgesamt) wurde die Operation vom Bedrohungsakteur bekannt gegeben, während 17 % (148 insgesamt) von Regierungsbehörden des betroffenen Staates gemeldet wurden.

Auch hier lassen sich Unterschiede nach der Art der Operation feststellen. Die meisten Operationen, bei denen es sich um Hijacking ohne Missbrauch handelt (60 %), wurden von IT-Sicherheitsunternehmen gemeldet, während die meisten Datendiebstähle und Datenlecks (48 %), die von ihrer Art her sehr sichtbar sind, direkt von den verantwortlichen Bedrohungsakteuren gemeldet wurden.

Quelle der Offenlegung von Cyberoperationen nach Art der Operation im Jahr 2023:



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

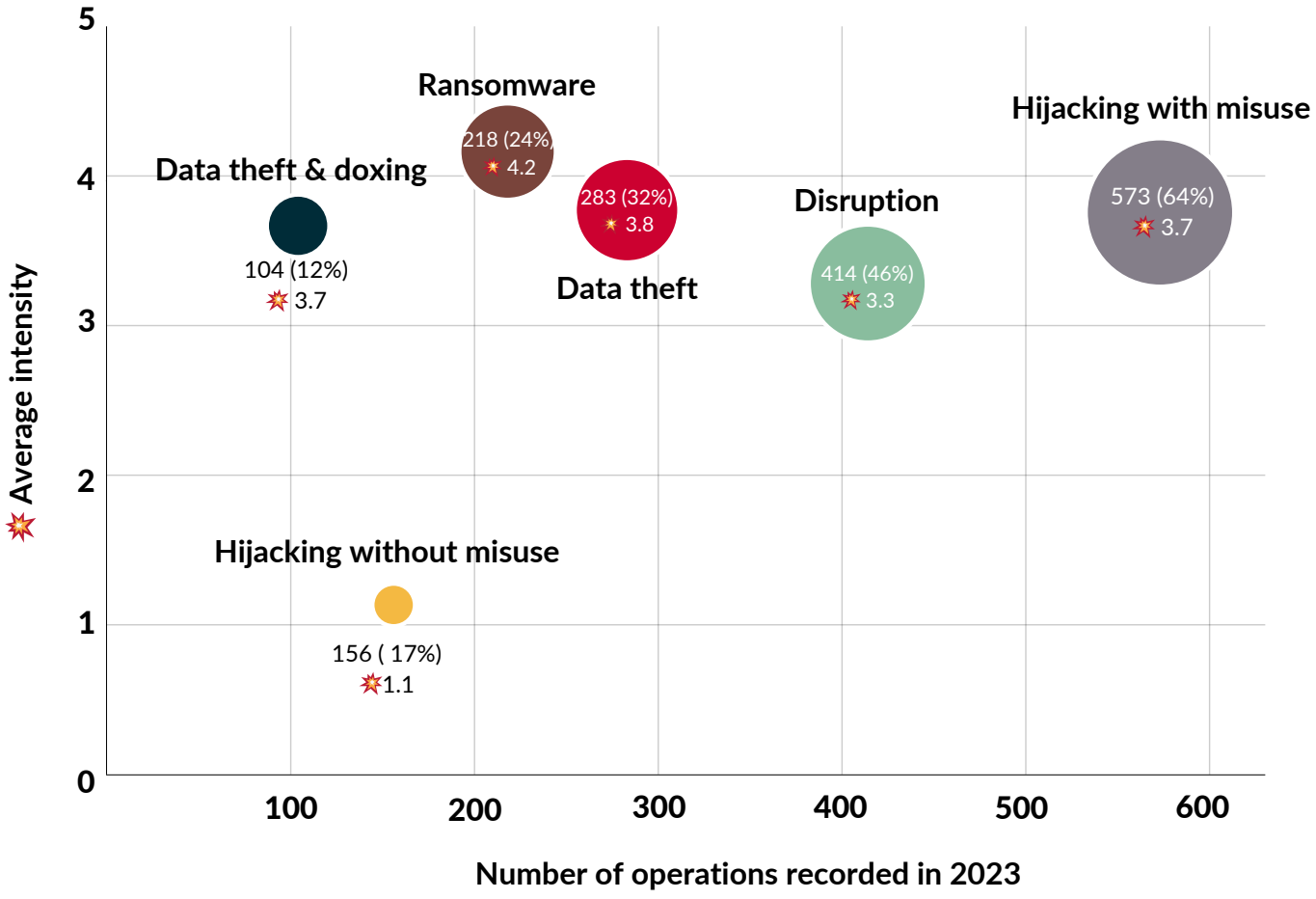
2 Verteilung der Operationen

2.1. Arten von Operationen und ihre Intensität

Im Jahr 2023 war die am häufigsten beobachtete Art von Cyberoperationen **Hijacking mit Missbrauch** mit insgesamt 573 Operationen (64 % aller Operationen). Fast die Hälfte (47 %) dieser Angriffe wurde mit Datendiebstahl verbunden (insgesamt 269). Die zweithäufigste Art waren **disruptive Angriffe** mit insgesamt 414 Vorgängen (46 % aller Vorgänge).

In Bezug auf die Intensität stachen jedoch Ransomware-Operationen mit dem höchsten durchschnittlichen Intensitätsgrad (4,2) heraus. Im Vergleich dazu waren weniger technisch anspruchsvolle Störungsoperationen wie DDoS-Angriffe und Defacements sowie Hijacking-Versuche, um sich ohne weiteren Missbrauch Zugang zu verschaffen, mit einem Durchschnittswert von 3,3 bzw. 1,1 weniger intensiv.

Verteilung der im Jahr 2023 erfassten Cyberoperationen nach Intensität:



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

Cyberoperationen von besonderer Intensität im Jahr 2023:

Sandworm nimmt den ukrainischen Energiesektor ins Visier, offenbar zeitgleich mit Raketenangriffen


Russian Sandworm group → 
Ukrainian critical infrastructure


Intensity score: 9


Disruption; Hijacking with misuse

Sandworm, ein Bedrohungsakteur mit einer bekannten Vielzahl von Angriffen auf kritische Infrastrukturen, infiltrierte ein ukrainisches Energieunternehmen und verursachte im Oktober 2022 einen Stromausfall inmitten russischer Raketenangriffe auf ukrainische Energieversorgungsunternehmen. Anschließend setzte Sandworm eine aktualisierte Version von CADDYWIPER gegen die IT-Umgebung des Opfers ein, um die Disruptionen zu verstärken und möglicherweise die Untersuchung des Vorfalls zu behindern. Die früheren Angriffe der Gruppe auf zivile Infrastrukturen waren Gegenstand eines förmlichen Ersuchens an den Chefankläger des Internationalen Strafgerichtshofs, eine Untersuchung wegen möglicher Kriegsverbrechen einzuleiten. Mit einem Intensitätswert von 9 übertrifft die Operation vom Oktober 2022 die durchschnittliche Intensität russischer staatlich gelenkter Gruppen gegen die Ukraine selbst in Kriegszeiten. In Anbetracht der Tatsache, dass Sandworm bereits vor diesem Raketenangriff die Möglichkeit hatte, die Operation durchzuführen, könnte die zeitliche Überschneidung auf Bemühungen hinweisen, den Einsatz konventioneller Waffen mit Cyberfähigkeiten zu kombinieren. Im Hinblick auf Cyber-Operationen kann diese Kombination auch den Vorteil bieten, die cyber-unterstützte Ursache des Stromausfalls zu verschleiern, und die Entdeckung von Angriffswegen und -werkzeugen zu verhindern. Regierungsbehörden in den USA, im Vereinigten Königreich und in der EU haben wiederholt eindeutige Verbindungen zwischen Sandworm und dem Hauptzentrum für Spezialtechnologien (GTsST), auch bekannt als Einheit 74455, die zum russischen Militärgeheimdienst GRU gehört, hergestellt.

2.2. Nutzung von Zero-Days

Bei 22 der im Jahr 2023 erfassten Cyberoperationen wurde eine Zero-Day-Schwachstelle ausgenutzt, wobei mehrere Zero-Days nutzten und 9 der Operationen im Jahr 2023 stattfanden. Dies entspricht dem Vorjahr, in dem sich 10 der Cyberoperationen, die 2022 stattfanden, auf Zero-Days stützten. Es dauerte im Durchschnitt 15 Monate, bis die im Jahr 2023 gemeldeten Vorfälle mit Zero-Days öffentlich zugeordnet werden konnten, das sind im Durchschnitt 5 Monate mehr als bei Vorfällen ohne Zero-Days.

Im Vergleich dazu dokumentierte Project Zero, eine Initiative von Sicherheitsforschern bei Google, welche die Nutzung nicht gemeldeter Schwachstellen verfolgt, für 2023 die Ausnutzung von 55 Zero-Days in freier Wildbahn. Dies bedeutet einen Anstieg um 34 % gegenüber 2022, aber einen Rückgang um 20 % gegenüber dem Allzeithoch von 69 Zero-Days, das Google für 2021 registrierte.

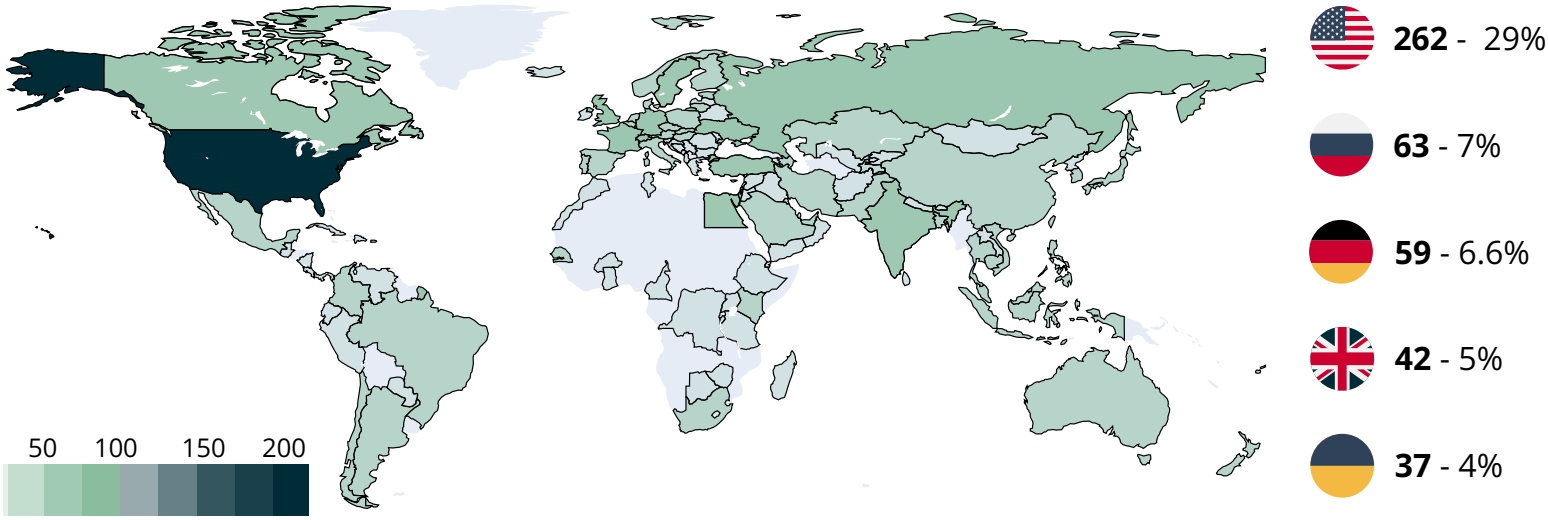
Die Überschneidung der Zero-Day-Nutzung zwischen den Daten von EuRepoC und Project Zero spiegelt den großen Anteil bisher unbekannter Schwachstellen bei Operationen gut ausgestatteter staatlicher Akteure sowie bei Operationen gegen gehärtete kritische Infrastrukturziele wider - Arten von Bedrohungsaktivitäten, die im Fokus der von EuRepoC durchgeführten Beobachtung von Vorfällen stehen.

3 Zielländer und -sektoren

3.1 Geografische Verteilung der Operationen

Im Jahr 2023 waren die **Vereinigten Staaten** mit 262 Vorfällen das Hauptziel von Cyberangriffen, viermal öfter als **Russland**, das mit 63 Vorfällen das am zweithäufigsten betroffene Land war. Auf die USA und Russland folgten **Deutschland** mit 59 Vorfällen, das **Vereinigte Königreich** mit 42 Vorfällen und die **Ukraine** mit 37 Vorfällen.

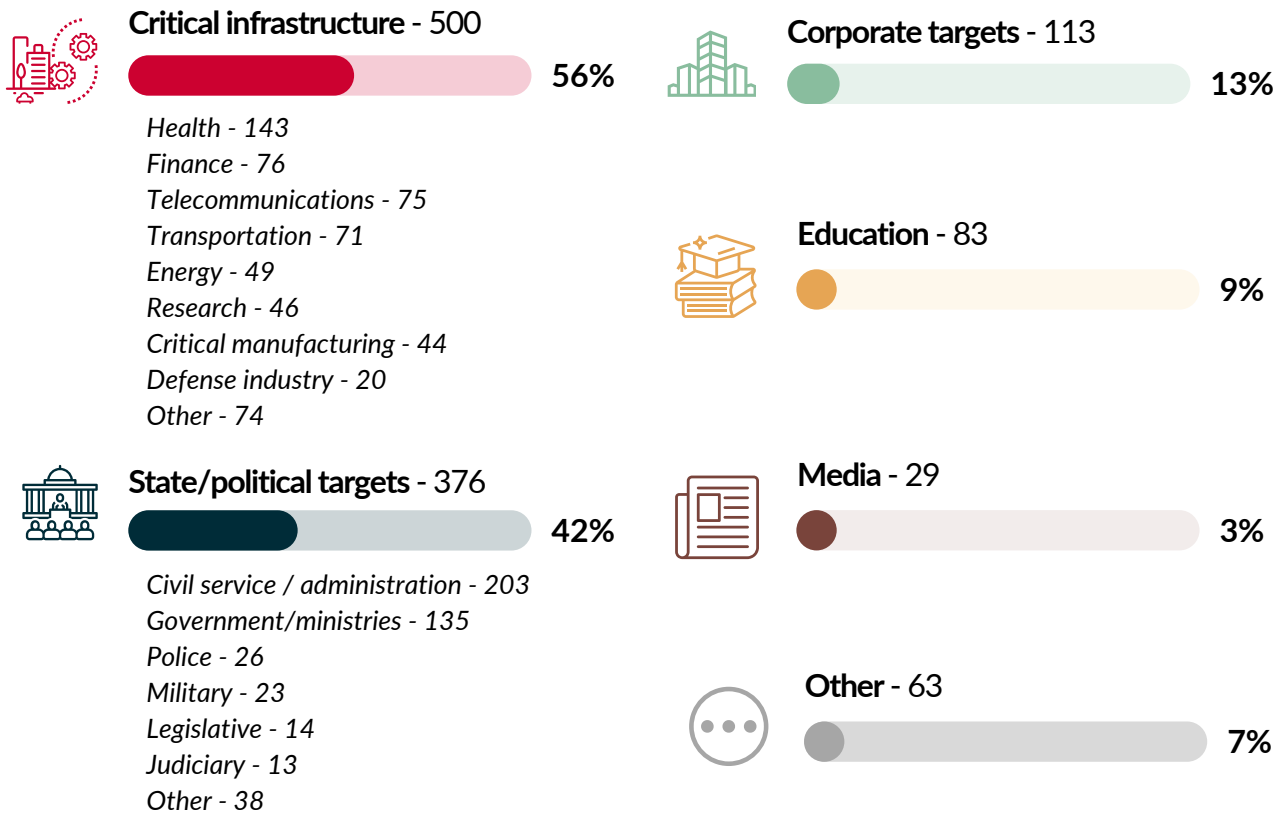
Anzahl der im Jahr 2023 erfassten Cyberoperationen nach Zielland:



3.2 Betroffene Sektoren

Mehr als **die Hälfte der im Jahr 2023 verzeichneten Cyberangriffe (56 %) zielten auf kritische Infrastrukturen** ab, insbesondere auf den Gesundheits-, Finanz- und Telekommunikationssektor. Auf den Gesundheitssektor entfielen 16 % aller neuen Cyberangriffe mit insgesamt 143 Vorfällen. **Staatliche Einrichtungen und politische Systeme** waren mit 42 % der neu erfassten Vorfälle der zweithäufigste Zielsektor. Die wichtigsten Unterkategorien waren der öffentliche Dienst und die Verwaltung mit 203 Vorfällen und Regierungen/Ministerien mit 135 Vorfällen.

Anzahl der Cyberangriffe nach Zielsektor im Jahr 2023:



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

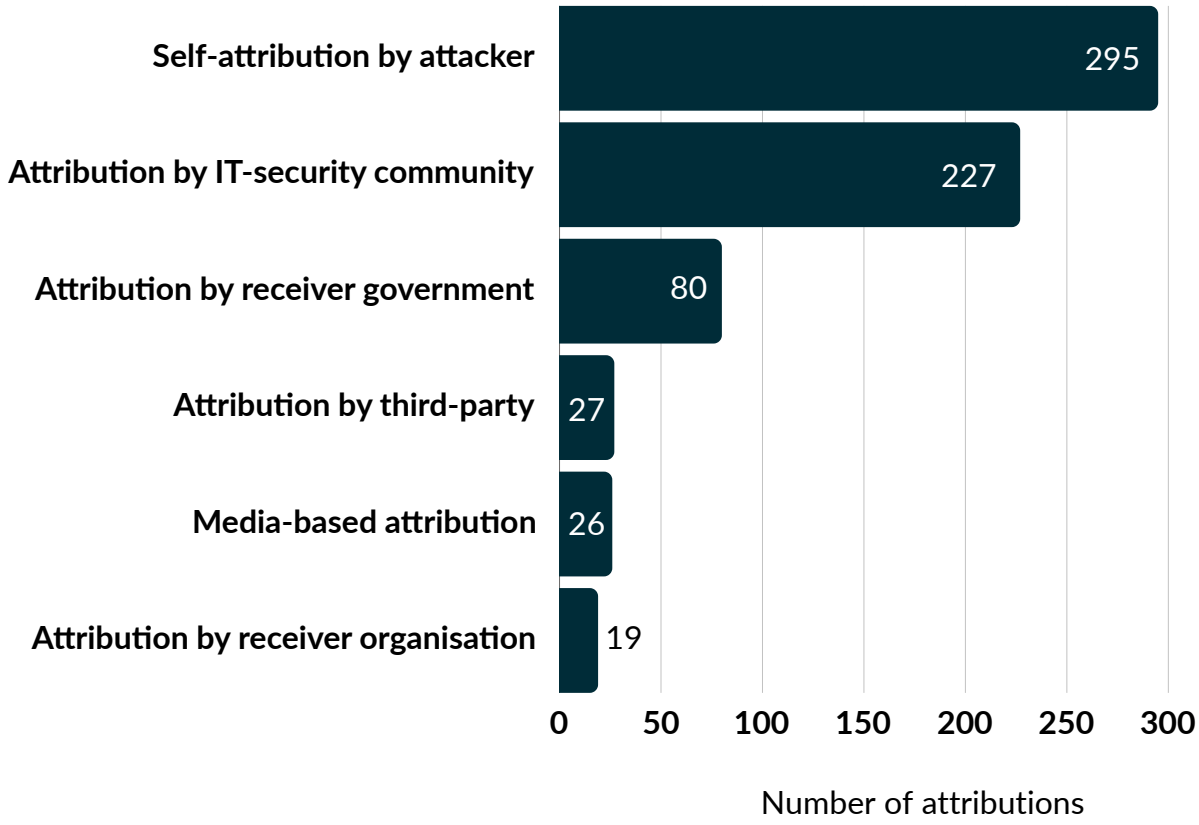
4 Attributionen und Angreiferprofile

4.1 Attribuierende Akteure

Fast zwei Drittel (65 %) der im Jahr 2023 erfassten Cyberoperationen wiesen mindestens eine öffentliche Attribution auf. Während für die meisten Vorfälle lediglich eine Attributionsaussage verzeichnet wurde, waren es bei einigen bis zu sechs verschiedene, so dass insgesamt 650 Verantwortungszuweisungen über alle Vorfälle hinweg erfasst wurden. In den meisten Fällen reklamierten die mutmaßlichen Angreifer die Operationen für sich selbst (45 % der Zuordnungen).

Selbstattributionen durch Ransomware-Gruppen oder Hacktivisten waren immer noch die häufigste Quelle für öffentliche Verantwortungszuschreibungen. Die IT-Sicherheits/Threat Intelligence-Community belegte mit 35 % der von EuRepoC im Jahr 2023 verzeichneten Attributionen den zweiten Platz.

Wer attribuierte 2023 am häufigsten?

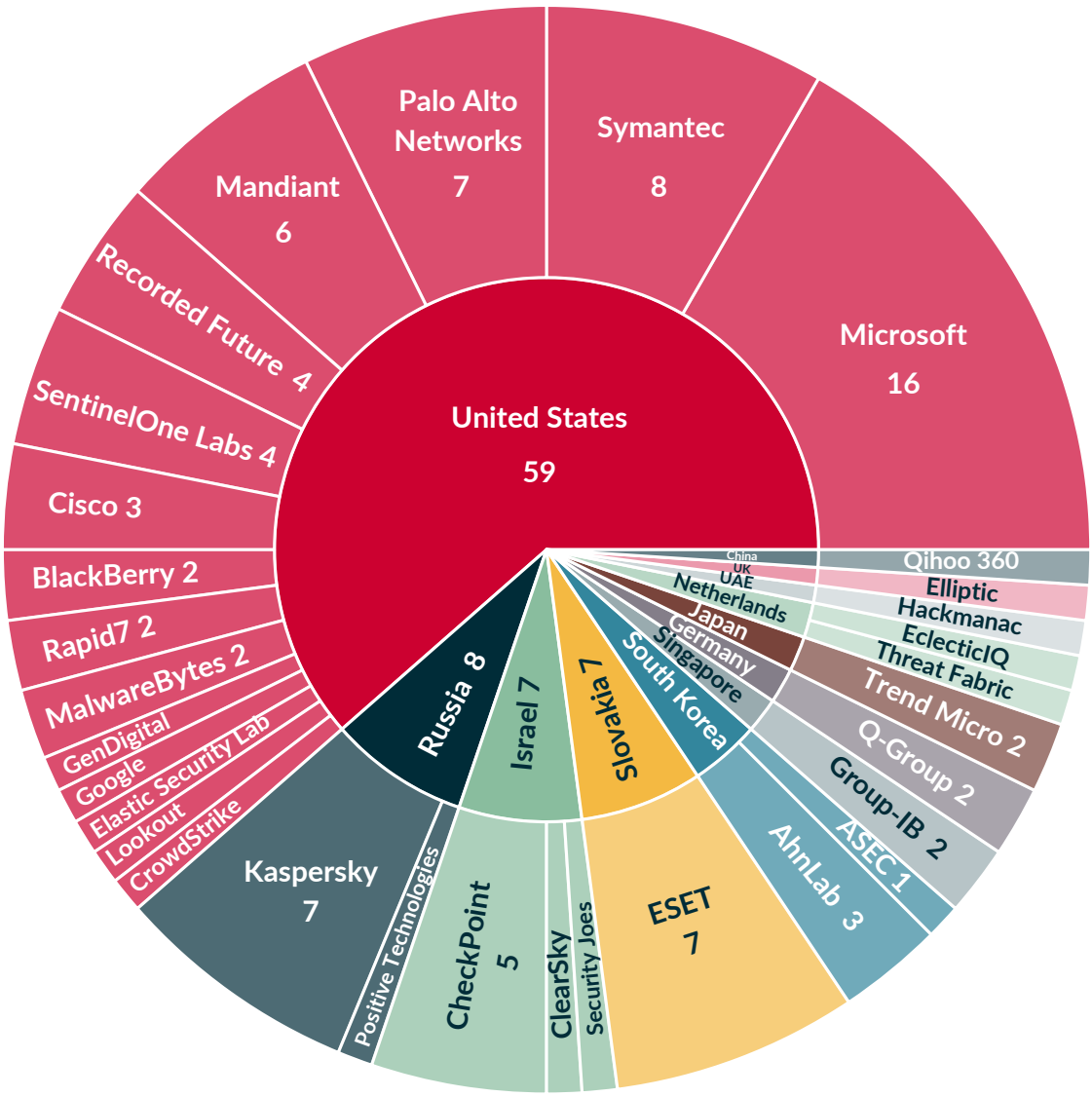


4.2 Attributionen durch IT/Threat Intelligence Unternehmen

Unter den IT/Threat Intelligence-Unternehmen verzeichnete EuRepoC für **Microsoft** 16 attribuierte Operationen, für **Symantec** 8, für **ESET**, **Kaspersky** und **Palo Alto Networks** jeweils 7 und für **Mandiant** 6.

Threat Intelligence-Unternehmen aus den **Vereinigten Staaten** liegen damit bei der Attribution weiter vorne, gefolgt von **Russland**, mit Kaspersky als dominierendem Unternehmen nach dem Rückzug von Group-IB, sowie Unternehmen aus der "Start-up-Nation" **Israel**.

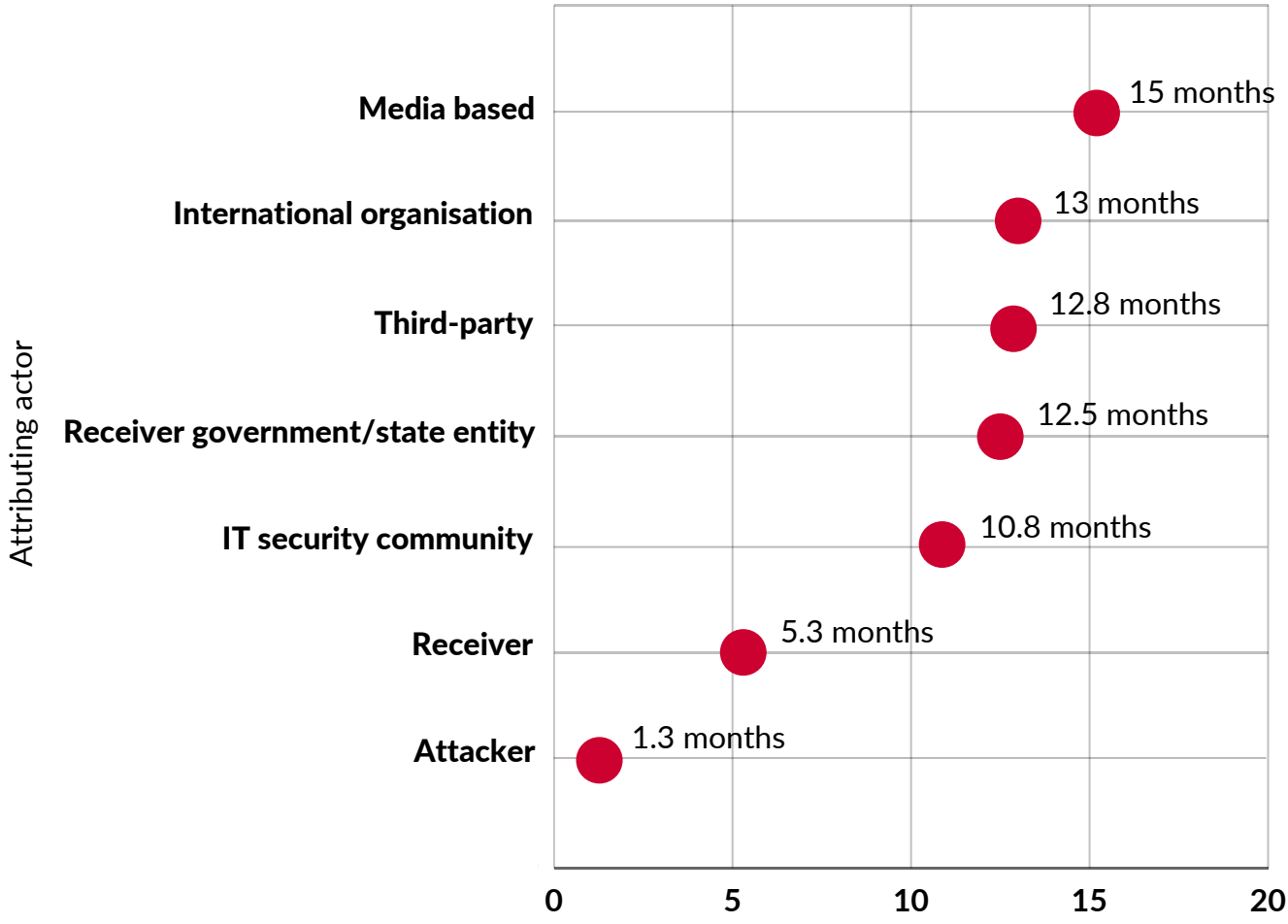
Anzahl an Operationen, die von IT/Threat Intelligence Unternehmen 2023 attribuiert wurden:



4.3 Attributionsgeschwindigkeit

Im Jahr 2023 wurden für alle erfassten Cyberoperationen **im Durchschnitt 10 Monate nach dem berichteten Startdatum der Operation öffentliche Attributionen vorgenommen**. Der Zeitrahmen für diese Zuschreibungen variierte erheblich, je nach Quelle der Attribution. Wenn die Angreifer die Verantwortlichkeit für eine Operation selbst reklamierten, erfolgte dies bereits innerhalb eines Monats. Im Gegensatz dazu dauerten Zuschreibungen aus Medienquellen bis zu 15 Monate. Darüber hinaus benötigten Regierungsstellen/staatliche Behörden im Durchschnitt 2 Monate länger als IT-/Threat Intelligence Unternehmen, um Cyberoperationen zu attribuieren, bei denen sie, beziehungsweise nationale Akteure das Ziel waren. Obwohl die Regierungen also immer noch mehr Zeit für öffentliche Attributionen benötigen, dürfte die durchschnittliche Zeitspanne zwischen technischer und politischer Verantwortungszuweisung in Zukunft weiter abnehmen.

Durchschnittliche Zeitspanne zwischen erfasstem Vorfallsstartdatum und öffentlicher Attribution:



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

4.4 Strittige und neue Attributionen

Nur fünf der im Jahr 2023 hinzugefügten Vorfälle enthielten strittige Zuordnungen/Informationen: Bei einer Cyberoperation ging es um die Leugnung der kolportierten Verantwortlichkeit durch die Ransomware-Gang Akira, aufgrund des angeblichen Hijackings ihrer Ransomware durch eine andere Gruppierung. Ein weiterer Vorfall wurde als ukrainische “False-Flag-Operation” bewertet, um die Verantwortung Mitgliedern der russischen Wagner-Gruppe zuzuschieben. Darüber hinaus wurden mehrere Cybervorfälle Anonymous Sudan zugeschrieben, deren selbsternannte Hacktivisten-Identität von Threat Intelligence-Unternehmen bestritten und stattdessen eine Verbindung zur russischen Gruppierung Killnet vermutet wird. Außerdem haben zwei Ransomware-Gruppen die Verantwortung für denselben Hack gegen Sony übernommen.

Die Attribution einer Cyberoperation ist oft ein fortlaufender Prozess, der mehrere Schritte umfasst und somit im Laufe der Zeit neue Informationen zur Charakterisierung des mutmaßlichen Bedrohungsakteurs hinzufügt. Entsprechend haben wir fünf neue Verantwortungszuschreibungen für bereits bestehende Vorfälle erfasst, die im Jahr 2023 gemeldet bzw. veröffentlicht wurden. Eine der fünf Attributionen betraf sogar zwei Vorfälle, die bereits 2015 und 2016 stattgefunden hatten und im jeweils folgenden Jahr veröffentlicht wurden. Wie Cybersicherheit im Allgemeinen sollte auch die Attribution von Vorfällen als Prozess und nicht als endgültiger Zustand betrachtet werden.

4.5 Politische Attributionen

Mit nur **12 % stammt ein relativ kleiner Teil der Attributionen von Regierungen oder staatlichen Behörden der Zielländer**. Die **Vereinigten Staaten** führten die Liste mit 28 Verantwortungszuweisungen an, gefolgt von der **Ukraine** (13), dem **Vereinigten Königreich** (7) und **Südkorea** (6). Dies entspricht auch der hohen Zahl der registrierten Cybervorfälle gegen Ziele aus den USA und der Ukraine im Jahr 2023.

Deutschland attribuierte öffentlich lediglich zwei der 59 im Jahr 2023 erfassten Vorfälle auf Ziele innerhalb des Landes. Das Bundesamt für Verfassungsschutz machte die nordkoreanische Hackergruppe Kimsuky für einen Vorfall gegen deutsche Forschungseinrichtungen im März 2023 verantwortlich. Das deutsche Innenministerium sprach der Ransomware-Gruppe "Akira" den Angriff auf den IT-Dienstleister Südwestfalen-IT vom 29. Oktober zu. Die Attributionsquote für deutsche Regierungsakteure/staatliche Behörden lag damit bei 3 %. Dies ist niedriger als auf Seiten Großbritanniens und der USA, mit einer Quote von 17 % bzw. 11 %.

4.6 Gemeinsam getätigte Attributionen

Bei einigen wenigen registrierten Cybervorfällen gab es "gemeinsame Verantwortungszuschreibungen" durch betroffene Regierungsstellen/Behörden mehrerer Länder. Diese Zuordnungscluster/Netzwerke können auf eine "Gleichgesinntheit", oder auch geteilte Normen/Werte bei der öffentlichen Attribution von Cyberangriffen hindeuten. Gleichzeitig erfordern gemeinsame Zuschreibungen ein gewisses Maß an Informationsaustausch, was ein erhebliches Maß an Vertrauen zwischen den Attributionspartnern widerspiegelt. Ferner ist bemerkenswert, dass die USA nicht nur zunehmend gemeinsame Erklärungen verschiedener inländischer Behörden veröffentlichen, sondern auch regelmäßig mit einem oder mehreren anderen Ländern zusammenarbeiten, um gemeinsame länderübergreifende Anschuldigungen vorzubringen. Diese Partnerländer, wie Japan, Südkorea oder die Ukraine, spiegeln regionale Brennpunkte wider, die sowohl im konventionellen als Cyberbereich von besonderer Bedeutung sind.

Cybervorfälle, die 2023 gemeinsam von Regierungen/staatlichen Stellen betroffener Länder attribuiert wurden:

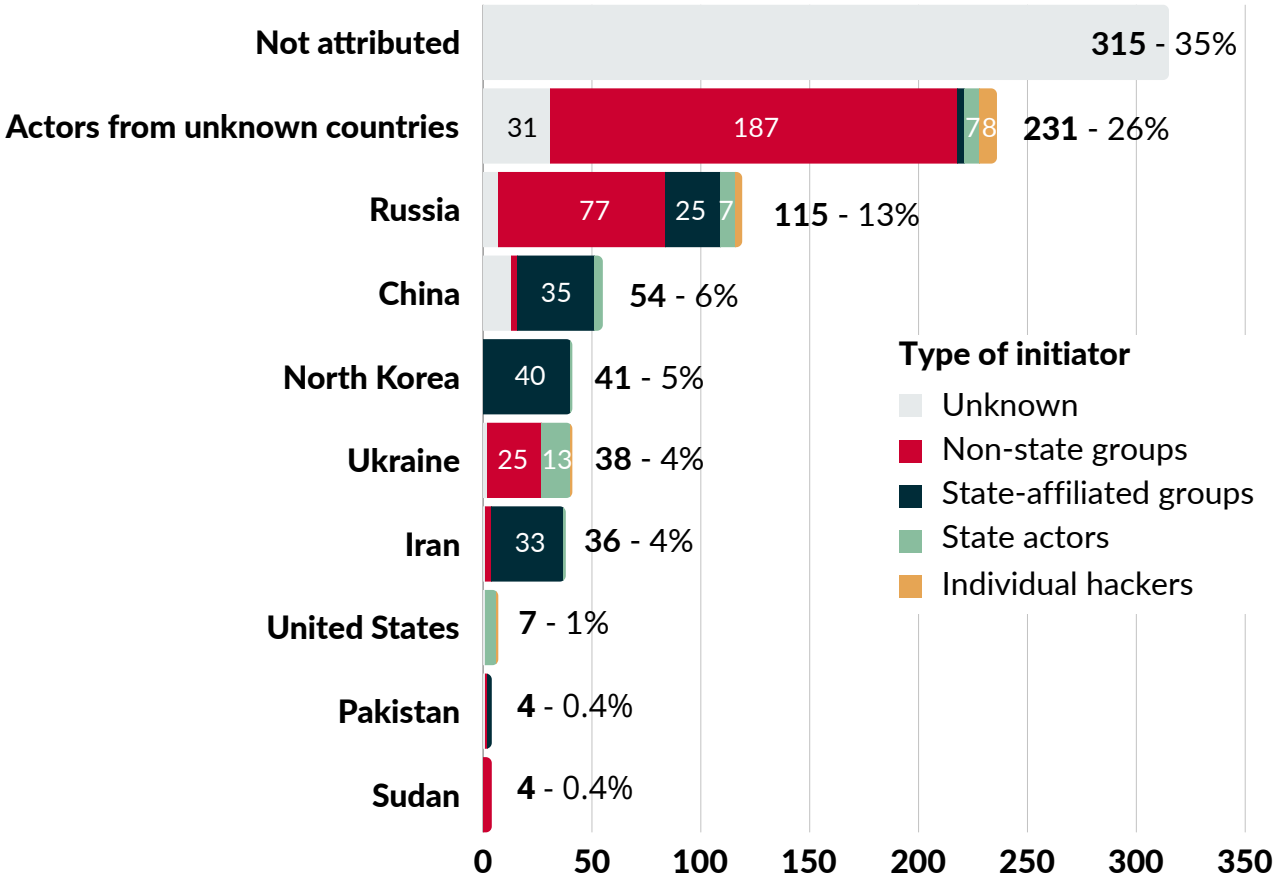
	2	-North Korean sponsored Andariel stole sensitive information from South Korean defense and pharmaceuticals companies and research institutes -Andariel disrupted US and South Korean healthcare providers and other critical infrastructure with ransomware attacks
	1	Chinese threat actor 'BlackTech' targeted 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 Vermuteter Ursprung der Cyberoperationen

35 % der im Jahr 2023 erfassten Operationen konnten bislang keinem Urheber zugeordnet werden, bei 26 % blieb das Herkunftsland bislang unbekannt. Eine beträchtliche Anzahl von Operationen (187 oder 21 %) wurde von **nichtstaatlichen Gruppen unbekannter Herkunft** initiiert.

Russische und **chinesische Hackergruppen** waren auch im Jahr 2023 am aktivsten: 13 % bzw. 6 % der Operationen wurden von Akteuren aus diesen beiden Ländern vorgenommen. In Russland handelte es sich dabei überwiegend um (formal) nichtstaatliche Gruppen (insbesondere NoName057(16) und Killnet), während in China ein erheblicher Teil staatlich organisierte/angeleitete Gruppen waren (65 % der von China aus initiierten Vorfälle), mit Mustang Panda und UNC 2814/Gallium als besonders aktiven Akteuren.

Vermutete Ursprungsländer der in 2023 erfassten Cyberoperationen:



4.8 Cyberoperationen von staatlichen und staatlich-affiliierten Angreifern

Staaten können mit ihren Cyberoperationen (oder denen ihrer Stellvertreter) unterschiedliche kurz- oder langfristige Ziele verfolgen. Im Falle Russlands spiegelt die Verteilung der in der EuRepoC-Datenbank erfassten Vorfallstypen die Dominanz von Operationen im Kontext des Krieges gegen die Ukraine wider, darunter Cyberspionage sowie disruptive Operationen wie Wiper-Angriffe, die in der Datenbank als eine Kombination aus "Hijacking with misuse" und "Disruption" kodiert werden. Im Gegensatz zu den ukrainischen Cyberoperationen ist es bemerkenswert, dass sich letztere im Jahr 2023 stärker auf Datendiebstahl und Doxing konzentrierten, einem Ansatzes folgender, der auf weitere Unterstützung der internationalen Öffentlichkeit sowie die Beeinflussung der russischen Öffentlichkeit bezüglich des Krieges abzielt, was in der Vergangenheit eine Taktik von russischem “Hack-and-Leak”-Angriffen war, nicht nur im Rahmen bereits eskalierter Konflikte.

Im Vergleich dazu wurden beispielsweise chinesische Cyberoperationen häufiger als "Hijacking without misuse" bewertet, d. h. als Infiltration von Zielsystemen, ohne dass weitere Auswirkungen gemeldet wurden. In Übereinstimmung mit früheren Berichten von Threat Intelligence Unternehmen spiegelt dies den chinesischen Ansatz wider, “Brückenköpfe” in strategisch wichtigen gegnerischen Netzwerken einzurichten, um im Falle einer Konflikteskalation in der Zukunft potenzielle Sabotage-Cyberoperationen gegen diese durchzuführen. Die vergleichsweise hohe Zahl solcher Fälle für iranische Akteure deutet auf eine potenziell ähnliche Taktik des Regimes in Teheran hin.

Vier der fünf erfassten Operationen mit Verantwortlichkeit staatlicher Akteure aus den USA wurden vom durchführenden Akteur selbst öffentlich gemacht: so machte das FBI seine zunehmenden Störoperationen gegen kriminelle und staatlich gesponserte Hacking-Netzwerke regelmäßig selbst öffentlich.

	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 Bedrohungsakteure

Im Jahr 2023 dominierten eindeutig Operationen von Hacktivisten im Kontext des russischen Krieges gegen die Ukraine, aber auch eine Vielzahl von Ransomware-Fällen, die von EuRepoC erfasst wurden. So gehören NoName057(16) und zwei prominente Ransomware-Gruppen zu den am häufigsten aufgenommenen Angreifern. Im Gegensatz dazu ist die nordkoreanische Lazarus-Gruppe eine staatlich gestützte/kontrollierte APT, deren hohe Aktivitätsrate die anhaltende Attraktivität von Cyberoperationen für das nordkoreanische Regime widerspiegelt, wie z. B. militärisch-technologisch motivierte Cyberspionage oder die Generierung finanzieller Ressourcen durch Hacks von Banken oder Krypto-Unternehmen. Auch bei den gemeldeten Cyberoperationen des ukrainischen Militärgeheimdienstes spielte die Selbstattribution eine wichtige Rolle, ebenso wie bei Hacktivisten und Ransomware-Operationen. Wenn Angreifer Anreize haben, ihre Operationen öffentlich zu machen, oder wenn der Erfolg der Operation selbst von deren öffentlichem Bekanntwerden abhängt, ist davon auszugehen, dass die absolute Operationsanzahl für diese Angreifer höher ist, als für Akteure, deren Operationen überwiegend im Verborgenen ablaufen.

Die aktivsten Angreifer im Jahr 2023

(*entsprechend der von EuRepoC erfassten Operationsanzahl*)

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, das von den Five Eyes-Staaten zusammen mit Frankreich und Deutschland als die weltweit aktivste Ransomware-Gruppe identifiziert wurde, ist der einzige Bedrohungsakteur, der sowohl zu den aktivsten Verursachern als auch zu den Akteuren gehört, für die das Repository die höchste durchschnittliche Intensität pro Operation im Jahr 2023 ermittelt hat. Ransomware-Gruppierungen dominieren das Intensitätsranking im Allgemeinen, was sich vor allem durch Berechnung des EuRepoC Intensitätsscore erklären lässt: Dieser hängt von der individuellen Intensitätsbewertung jedes kodierten Vorfallsarten (incident type) für eine Gesamtoperation ab, und da Ransomware-Operationen oft nicht nur Disruption und Hijacking with Misuse, sondern im Falle von "double extortion" auch Data Theft (und manchmal Doxing) umfassen, führt dies aufgrund der höheren Anzahl kodierter Vorfallsarten oft auch zu einer höheren Gesamtintensitätsbewertung. Dies spiegelt jedoch gleichzeitig die Komplexität und Flexibilität von Ransomware als Erpressungsmethode wider. In öffentlichen Berichten wurde bereits auf die "triple extortion"-Methode hingewiesen, bei der die Angreifer die Kunden oder Partner des Zielunternehmens kontaktieren und sie über die potenzielle Offenlegung ihrer Daten informieren, falls das Zielunternehmen/der betroffene Akteur sich weigert das Lösegeld zu zahlen, mit dem Ziel, dessen Druck zu erhöhen. Bei der "quadruple extortion" wird dann zusätzlich damit gedroht, die Server/Netzwerke des Opfers mit einem DDoS-Angriff lahmzulegen, falls die Lösegeldzahlung verweigert wird. Die Benachrichtigung von Behörden durch Ransomware-Gruppierungen über die angebliche Verletzung von Offenlegungsregeln durch ihre Opfer könnte sogar zu einer weiteren Ransomware-Evolution führen. Bei den staatlich gesponserten APTs überrascht es nicht, dass Sandworm die Gruppe mit der höchsten durchschnittlichen Intensitätsbewertung ist. Bereits seit vielen Jahren agiert die Gruppe im Einklang mit den militärischen Zielen des russischen Geheimdienstes GRU, insbesondere gegen ukrainische Ziele und oft mit physischen Auswirkungen, was insgesamt im Cyberkonfliktaustrag immer noch eher selten ist.

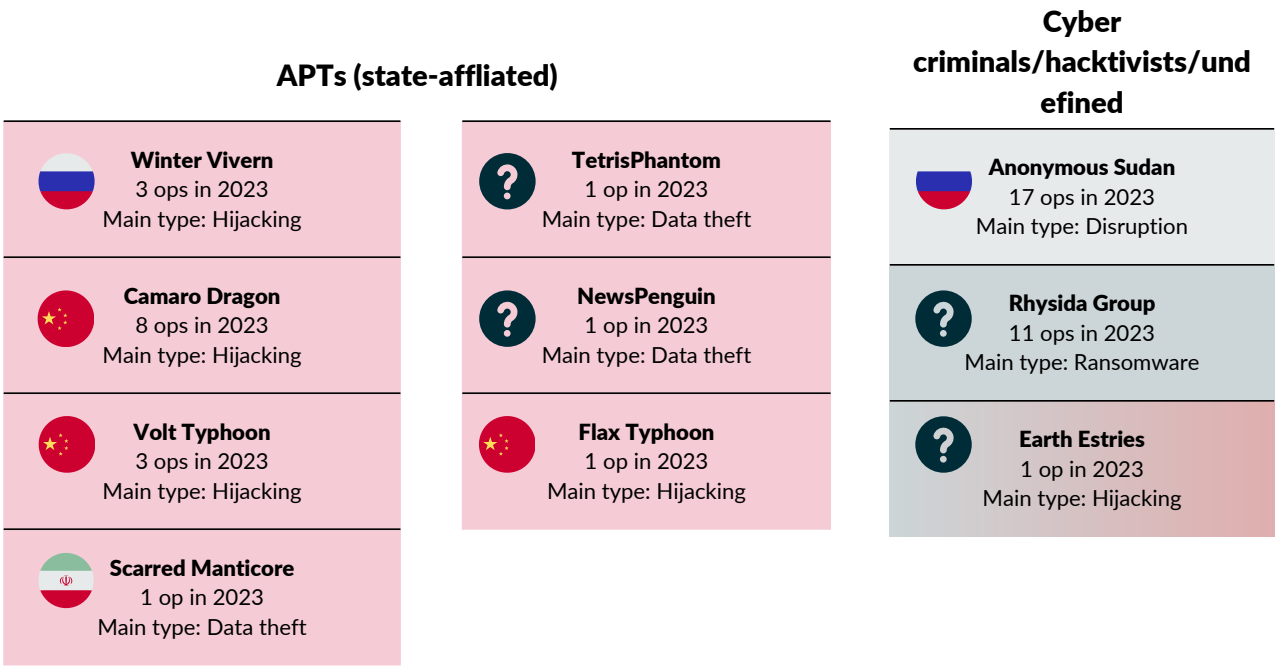
Angreifer mit den durchschnittlich intensivsten/schwerwiegendsten Cyberoperationen erfasst im Jahr 2023:

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 “Newcomer” im Jahr 2023

Im Jahr 2023 traten auch **neue Angreifergruppen** auf, die zuvor nicht in der EuRepoC-Datenbank erfasst waren. Drei der sieben erstmals erfassten APTs wurden China als staatlichem Sponsor zugeschrieben, gefolgt von einer neuen russischen und iranischen Gruppe, denen ebenfalls staatliche Verbindungen zugesprochen wurden. Diese Beobachtung spiegelt das florierende chinesische Cyber-Ökosystem wider, in dem es einerseits zu einem verstärkten Austausch/Teilen von Angriffswerkzeugen zwischen staatsnahen Gruppen kommt, andererseits aber auch zu einer Ausweitung der delegierten Aufgaben im Cyber-Raum, was zur Bildung weiterer Hackergruppen führte.

Da sich auch das Ransomware-Ökosystem immer weiter ausbreitet und Gruppen sich neu organisieren, um die Strafverfolgung zu erschweren, erfasste EuRepoC auch Ransomware-Operationen einer Cybercrime-Gruppierung, deren Aktivitäten in den Jahren zuvor noch nicht berichtet wurden. Wie so oft bei Ransomware-Gruppen gehen die Einschätzungen jedoch auseinander, ob es sich bei Rhysida tatsächlich um eine neue Gruppe mit eigenen Mitgliedern handelt, oder ob die bereits seit 2021 aktive Gruppe Vice Society die Ransomware Rhysida lediglich erst ab Mai 2023 einsetzt.



5 Politischer und rechtlicher Kontext

5.1 Verbindungen zu bestehenden konventionellen Konflikten

Im Jahr 2023 durch EuRepoC erfasste Cyberoperationen, die bestehenden konventionellen Konflikten zugeordnet werden konnten:

	**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

Die aufgeführten Konfliktdyaden spiegeln einen bereits etablierten Befund der Cyberkonfliktforschung wider, nämlich dass Cyberoperationen häufig im Kontext regionaler und damit oft bereits gewaltsam eskalierter Konflikte (auch "Enduring Rivals" genannt) eingesetzt werden, auch wenn sie meist nur zusätzlich zu konventionellen militärischen Mitteln und nicht als Ersatz hierfür eingesetzt werden.

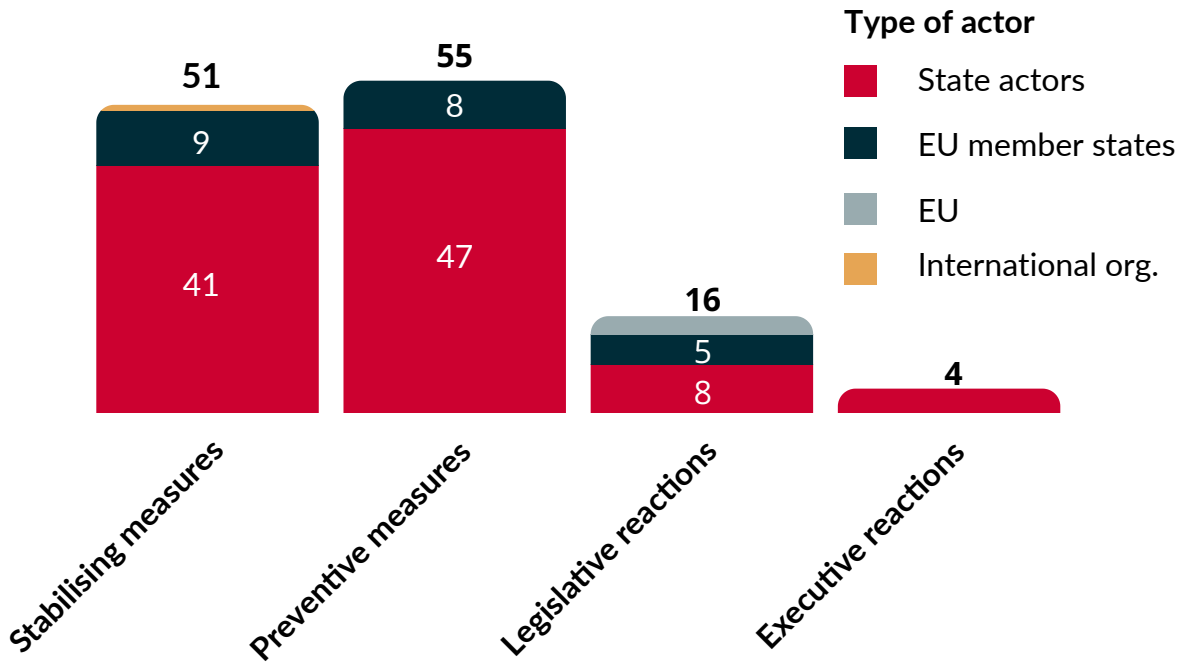
Der russische Krieg gegen die Ukraine war die Ursache für 16 % der im Jahr 2023 erfassten Operationen. Davon waren 37 % (insgesamt 52) entweder gegen Russland oder die Ukraine selbst gerichtet, wobei 35 Vorfälle (25 %) von ukrainischen Gruppen gegen russische Ziele und 17 (13 %) von russischen Gruppen gegen ukrainische Ziele initiiert wurden. Ein ähnlicher Anteil dieser Operationen (38 % bzw. 51 insgesamt) wurde von Gruppen russischen Ursprungs (hauptsächlich formal nichtstaatlichen Gruppen) gegen Länder durchgeführt, die die Ukraine unterstützen, insbesondere die USA und EU-Mitgliedstaaten.

Der Konflikt zwischen Iran und Israel liegt zahlenmäßig weit abgeschlagen an zweiter Stelle, gefolgt vom Konflikt zwischen Israel und Hamas, in welchem Cyberaktivitäten vor allem nach der gewaltsamen Eskalation am 7. Oktober erfasst wurden. Es ist schwer einzuschätzen, ob und wenn ja, welche iranischen Cybervorfälle gegen israelische Ziele als Solidaritäts- bzw. Unterstützungsaktionen für die Hamas durchgeführt wurden, da zwischen Iran und Israel seit langem disruptive Stör- und Spionageaktionen stattfinden. Angesichts der bemerkenswerten Zunahme der aufgezeichneten Operationen aus dem Iran gegen israelische Ziele seit dem 7. Oktober scheinen zumindest einige damit verbundene Cyber-Aktivitäten plausibel zu sein.

5.2 Politische Reaktionen

Im Jahr 2023 lösten insgesamt **108 Cybervorfälle (12 % aller erfassten Ereignisse) eine politische Reaktion aus**. Diese wurden wie folgt eingeteilt:

Types of political responses in 2023:



Note: Individual cyber incidents may have multiple political responses.

Stabilisierende Maßnahmen meinen Erklärungen von Regierungsvertretern oder Vertretern internationaler und supranationaler Organisationen, während sich präventive Maßnahmen auf die Sensibilisierung durch Cybersicherheitsbehörden wie das US-amerikanische CISA, das ukrainische CERT-UA oder das deutsche BSI beziehen. Dazu gehören auch Initiativen zur Vertrauensbildung oder dem Aufbau von Kapazitäten von Staaten in Drittländern, welche in der Datenbank möglicherweise unterrepräsentiert sind, da sie nur gelegentlich öffentlich bekannt werden oder nicht als konkrete Reaktion auf einen bestimmten Vorfall benannt werden (Beispiele siehe hier und hier). Bei den legislativen Maßnahmen handelt es sich größtenteils um Äußerungen von Oppositionsmitgliedern oder die Bildung parlamentarischer Untersuchungsausschüssen. Die Klassifizierung durch EuRepoC basiert auf der EU Cyber Diplomacy Toolbox (CDT). Während es sich rechtlich um Instrumente der EU und ihrer Mitgliedstaaten handelt, erlaubt die Verwendung der CDT als Bewertungsrahmen jedoch einen Vergleichsmaßstab, wenn es um die Einschätzung zu Maßnahmen von Drittstaaten geht.

Die **Vereinigten Staaten** waren mit politischen Reaktionen zu 35 Operationen führend. Bei den meisten dieser Reaktionen handelte es sich um Präventivmaßnahmen (24), gefolgt von stabilisierenden Reaktionen (10). Die politischen Reaktionen der **Ukraine** betrafen 10 Vorfälle, ausnahmslos Warnungen des CERT-UA als Präventivmaßnahmen. **Deutschland** reagierte auf insgesamt 10 Vorfälle mit unterschiedlichen politischen Maßnahmen, darunter legislative Maßnahmen (6), die hauptsächlich einen DDoS-Angriff im April 2023 betrafen, präventive Maßnahmen (4) und stabilisierende Maßnahmen (3).

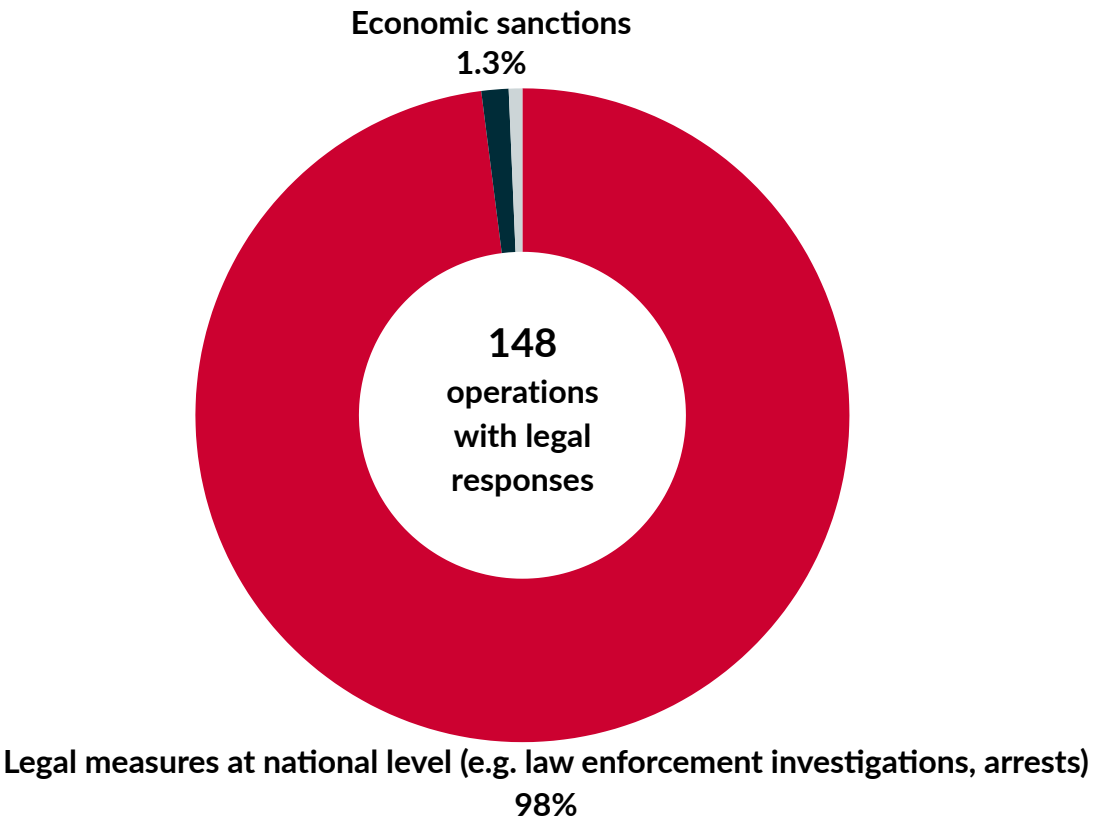
5.3 Rechtliche Reaktionen

16,5% (insgesamt in 148 Vorfällen) der im Jahr 2023 erfassten Cyber-Operationen kam es zu einer rechtlichen Reaktion. Bei diesen Reaktionen handelte es sich überwiegend um Maßnahmen auf nationaler Ebene (98 %). Bei den meisten Maßnahmen handelte es sich um Meldungen, dass Ermittlungen der Strafverfolgungsbehörden eingeleitet wurden. Nur bei wenigen Vorfällen hat EuRepoC im Jahr 2023 Verhaftungen und anschließende Gerichtsverfahren aufgenommen, was zeigt, wie schwierig die effektive Rechtsverfolgung für Staaten ist. Die Strafverfolgungsbehörden hatten jedoch einigen Erfolg mit der koordinierten Zerschlagung der Infrastruktur Cyberkrimineller, wie die Fälle Qakbot und ALPHV/BlackCat beispielhaft zeigen.

Zwei Vorfälle führten zu wirtschaftlichen Sanktionen durch die Vereinigten Staaten. Die entsprechenden Vorfälle wurden von der vom russischen Staat gesponserten Callisto-Gruppe zugeschrieben, die ab Mai 2022 eine Spearphishing-Kampagne gegen das US-Energieministerium und ab April 2022 gegen mehrere US-Verteidigungseinrichtungen durchführte. In beiden Fällen verfolgte Callisto wahrscheinlich Spionagezwecke. Darüber hinaus verhängten das Vereinigte Königreich und die USA im Dezember 2023 gemeinsam Sanktionen gegen die Gruppe wegen Einmischung in demokratische Prozesse im Vereinigten Königreich.

An der Spitze der Länder, die rechtliche Schritte einleiteten, standen die Vereinigten Staaten (61), gefolgt von Deutschland (11), Frankreich (9) und dem Vereinigten Königreich (8).

Types of legal responses in 2023:



Bemerkenswerter Vorfall:

Im April 2023 griff die Ransomwaregruppe Play den Schweizer IT-Dienstleister Xplain AG an

Play ransomware group → **Swiss IT provider**

Intensity score: 5

Ransomware

Im April 2023 griff die Ransomwaregruppe Play den Schweizer IT-Dienstleister Xplain AG an. Dabei wurden Daten des Unternehmens verschlüsselt und gestohlen sowie im Anschluss vollständig veröffentlicht, ein für Play übliches Vorgehen, sofern keine Lösegeldzahlung erfolgt. Außergewöhnlich machte den Vorfall, dass die Xplain AG für einen Großteil der Schweizer Behörden IT-Lösungen bereithält und im Zuge der Veröffentlichung als streng geheim eingestufte Informationen bekannt wurden. Auf den Vorfall wurde auf politischer Ebene durch die Einrichtung eines Krisenstabs reagiert, auf juristischer Ebene dauern die Ermittlungen der Schweizer Sicherheitsbehörden sowie des Datenschutzbeauftragten an. Der Vorfall wurde von uns mit einem in diesem Jahr unerreichten Impact Score von 14 bewertet, der anhand der Kriterien der Cyber Diplomacy Toolbox der EU die Schwere eines Cybervorfalls aus politischer und rechtlicher Sicht ermitteln soll. Der Fall zeigt die Abhängigkeit von staatlichen Institutionen und privaten Unternehmen durch externe Dienstleister, die im Rahmen von "Supply-Chain"-Attacken für verschiedene Bedrohungsakteure lukrative Ziele darstellen.

Mehr von EuRepoC

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

Über die Autor:innen

Jakob Bund ist Wissenschaftler an der Stiftung Wissenschaft und Politik (SWP).

Kerstin Zettl-Schabath ist Wissenschafterin am Institut für Politische Wissenschaft (IPW) der Universität Heidelberg.

Martin Müller ist Universitätsassistent und Dissertant am Institut für Theorie und Zukunft des Rechts an der Universität Innsbruck.

Camille Borrett ist Datenanalystin an der Stiftung Wissenschaft und Politik (SWP).