European
Repository of
Cyber Incidents

EuRepoC

Cyber Conflict Briefing

April 2024

Jakob Bund
Kerstin Zettl-Schabath
Martin Müller
Camille Borrett (Data Support)

Beobachtungen zur Gesamtlage

Im **April 2024** wurden 94 Cyber-Operationen in die EuRepoC-Datenbank aufgenommen. Das sind 32,4% mehr als im Vormonat und 22 Operationen mehr als die insgesamt durchschnittlich verzeichnete Aktivität von 72 Cyber-Operationen pro Monat im Gesamtzeitraum.

Die **durchschnittliche Intensität** der im April 2024 erfassten Operationen beträgt 3,24 und liegt somit über dem historischen Durchschnitt (2,82). Der auffällige Anstieg der Operationen seit Februar 2023 lässt sich vor allem auch dadurch erklären, dass EuRepoC ab diesem Zeitpunkt Cyberangriffe gegen Kritische Infrastrukturen grundsätzlich miteinschließt und nicht wie zuvor davon abhängig macht, ob diese Aktivitäten mit politischen beziehungsweise staatlichen Angreifern oder Opfern verknüpft sind.

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 notwendigerweise im April stattgefunden haben, sondern können bereits zu einem früheren Zeitpunkt begonnen haben. Dabei stehen technische, politische sowie rechtliche Aspekte im Vordergrund.

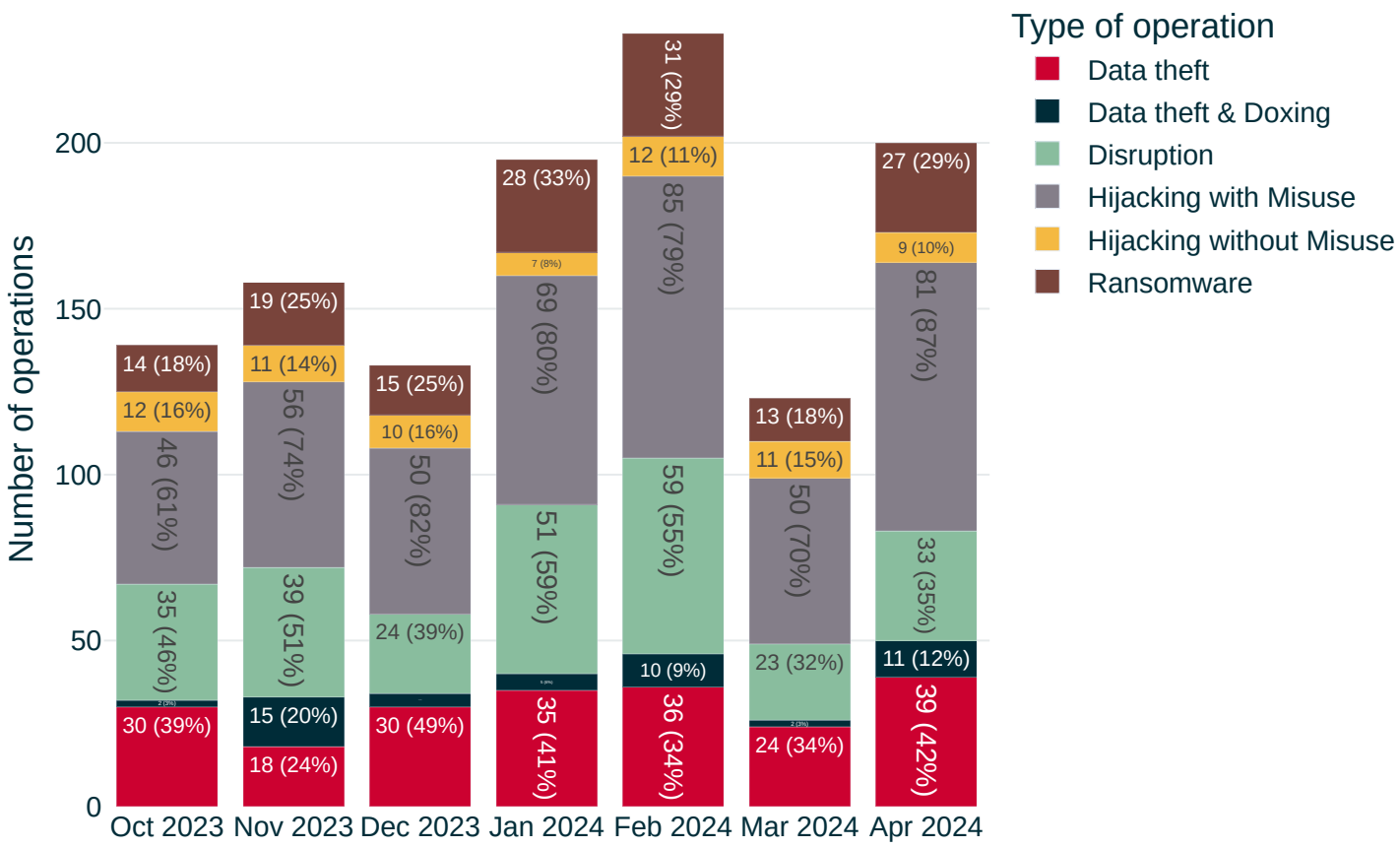
Über EuRepoC

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.

Die im April 2024 erfassten Vorfälle verteilen sich auf folgende **Operationstypen**:

Monthly distribution of operations



Hinweis: Einzelne Cybervorfälle können mehrere Operationstypen in Kombination aufweisen.

Der größte Anteil umfasst „Hijacking with Misuse"-Operationen mit 81 Fällen (87%). Der zweithäufigste im April 2024 festgestellte Operationstyp war 'Data theft'-Operationen (42%). Von diesen Operationstypen sind für April 2024 39 durch das Repositorium erfasst.

Wie im vorausgehenden Briefing für März beobachtet, stellen die Entwendung und Löschung von betriebswichtigen Daten nicht nur für kriminelle Akteure mit finanziellen Interessen ein Druckmittel dar. Hacktivistische Gruppierungen bedienen sich dieser Werkzeuge ebenfalls zur Durchsetzung politischer Ziele. Im April setzten die Cyber-Partisans, ein hacktvisitische Gruppe, die sich 2020 in Opposition zu weiter repressiven Entwicklungen des Lukaschenko-Regimes in Belarus gebildet hat, diese Taktik ein. Die Gruppe verschlüsselte mehrere hundert Arbeitscomputer und löschte Datenbanken, Backups und E-Mailspeicher von Hrodna Azot, einem der größten Betriebe des Landes. Das Kollektiv verschaffte sich außerdem Zugang zu den Überwachungssystemen des Chemiekonzerns.

Zuvor hatten Mitglieder der Cyber-Partisans über mehrere Monate hinweg die Netzwerke des Unternehmens aufgeklärt. Nach eigenen Angaben gelang der Gruppe ein weitreichender Zugriff auf Kontrollsysteme mit der Möglichkeit, die Produktion des Werks insgesamt einzustellen.

Um Kollateralschäden für Mitarbeitende und langanhaltende Auswirkungen für die Bevölkerung durch einen Produktionsausfall auszuschließen, schalteten Angehörige der Gruppe stattdessen die Heizzentrale ab – ein System, von dem sie wussten, dass es Ersatzquellen gab.

Im Gegenzug dafür den Zugang zu blockierten Systemen wiederherzustellen, forderten die Cyber-Partisans die Freilassung von Mitarbeitenden des Konzerns und 75 weiteren politischen Gefangenen, die sich in bedenklichem medizinischen Zustand befinden. Nach Protesten gegen die offiziellen Wahlergebnisse, die Lukashenko 2020 eine sechste Amtszeit als Präsident zusprachen, waren wiederholt Arbeiter und Arbeiterinnen des Werks festgenommen worden, begleitet von Einschüchterungsmaßnahmen und politisch motivierten Kündigungen durch die Konzernleitung. Vor diesem Hintergrund belegten die USA und die EU 2021 Hrodna Azot mit Sanktionen, denen sich Japan und die Ukraine 2022 anschlossen.

Mit Bezug auf diese Schritte bezeichnete die Cyber-Partisans ihre Aktionen gegen Hrodna Azot als Cyber-Sanktionen. Andere an der politischen Unterdrückung beteiligte Unternehmen und Organisationen stellen nach Auffassung der Gruppe ebenfalls ein Ziel dar.

In der eigenen Darstellung unterstrich die Gruppe, die Zurückhaltung von Fähigkeiten. Sollten die Forderungen unerfüllt bleiben, warnte die Gruppe vor einem verstärkten Einsatz.

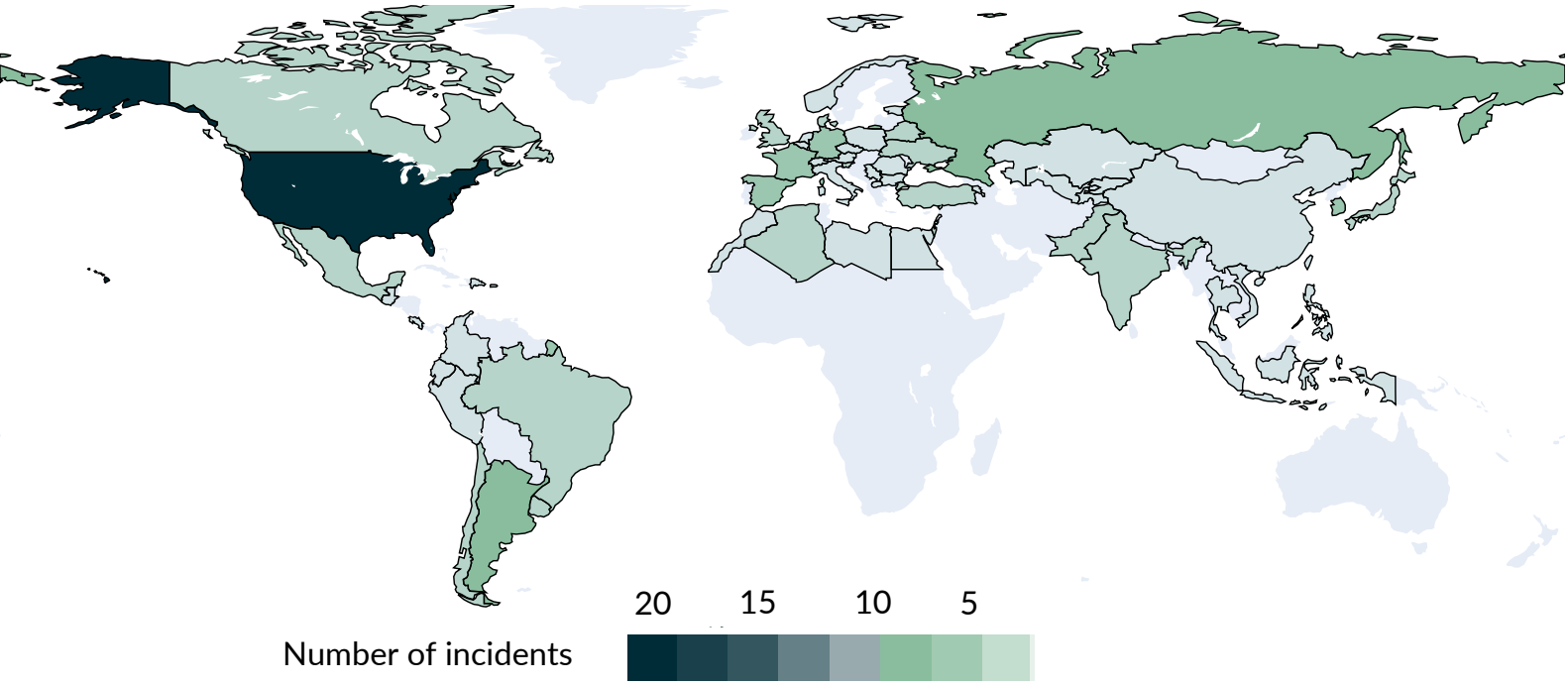
Um dieser Ankündigung und der Forderung nach der Freilassung Nachdruck zu verleihen, aktivierten die Cyber-Partisans am 3. Mai die zeitgesteuerte Löschung weiterer Daten von Servern in Netzwerken, die Hrodna Azot vermeintlich gesichert hatte.

Brennpunkte und Zielmuster

Unternehmen der kritischen Infrastruktur waren im April mit 54 Vorfällen am häufigsten betroffen, was 57% der neu aufgenommenen Fällen entspricht. Danach waren in 42 Fällen bzw. 45% staatliche Institutionen am zweithäufigsten betroffen. Nach dem deutlichen Rückgang an Fällen für den März handelt es sich gegenüber dem Februar damit um Anstiege sowohl für kritische Infrastrukturen (plus 64%) als auch für staatliche Institutionen (plus 17%).

Die Vereinigten Staaten waren im April mit 24 Vorfällen erneut am häufigsten betroffen. Ähnlich oft waren es Mitgliedstaaten der Europäischen Union, für die 23 Fälle aufgenommen wurden. Im Vergleich zum Vormonat März blieben die Zahlen annähernd identisch. Im Gegensatz stieg die Zahl der Vorfälle für Ziele außerhalb der EU und den USA. So waren etwa nach den Vereinigten Staaten Russland und Argentinien von jeweils sieben Vorfällen betroffen, bevor Deutschland und Spanien mit sechs Vorfällen zwei europäische Staaten folgen.

Geographic distribution of operations



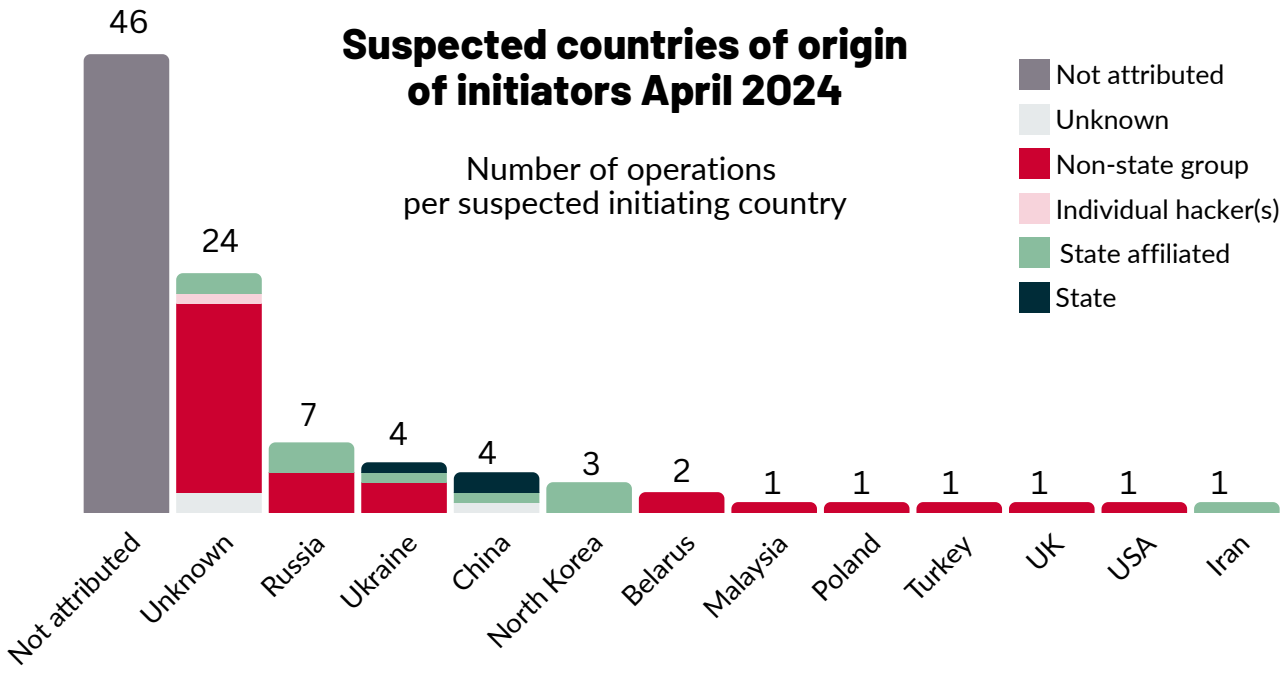
Von den betroffenen kritischen Infrastrukturen waren mit 17 Vorfällen fast ein Drittel im Gesundheitssektor, davon die Hälfte in den Vereinigten Staaten. Sensible Gesundheitsdaten machen den Sektor besonders anfällig für Datendiebstähle, die im April elf der Vorfälle betrafen. Wenngleich die Attribution in vielen Fällen (noch) aussteht, zeigen sich bei den bekannten Verursachern fast ausschließlich Ransomwaregruppierungen.
Am zweithäufigsten betroffen war der Bereich der kritischen Fertigung in acht Vorfällen. Auch hier sind kriminelle Gruppen zu nennen, die den Sektor im Visier haben. Aufgrund der bedeutenden Rolle von geschützten Verfahrenstechniken ist aber auch Industriespionage ein zusätzlicher Faktor, der gerade in Deutschland durch den Diebstahl von Daten beim Volkswagen-Konzern öffentlich bekannt wurde und staatlichen chinesischen Akteuren zugerechnet wird. Weiterhin häufig betroffen waren der Bereich digitaler Dienstleister und der Finanzsektor mit sechs Vorfällen. Im Bereich der Dienstleister spielten Ransomwaregruppen etwa bei Vorfällen in der Schweiz und Chile ebenso eine Rolle wie staatliche Akteure bei der Ausnutzung einer Zero-Day-Schwachstelle des IT-Sicherheitsunternehmens Palo Alto Networks. Im Finanzsektor, welcher in den vergangenen Monaten verstärkt im Zusammenhang mit Diebstählen von Kryptoplattformen in die Datenbank aufgenommen wurde, war im April durch disruptive Angriffe oder solche kriminell operierenden Gruppierungen betroffen.

Bei den staatlichen Institutionen fällt erneut auf, dass überdurchschnittlich oft regionale und lokale Behörden betroffen sind - im April waren es etwa zwei Drittel der Vorfälle, in denen staatliche Institutionen Opfer von Cybervorfällen waren. Diese Beobachtung entspricht der Annahme, dass lokale gegenüber nationalen Einrichtungen mit den verfügbaren Ressourcen ein geringeres Schutzniveau erreichen, das insbesondere von kriminellen Akteuren aus Opportunitätsgründen ausgenutzt wird. Allerdings muss hier auch genannt werden, dass bei ebenfalls fast zwei Dritteln der Vorfälle die Urheber aktuell nicht öffentlich bekannt sind. Bei den nationalen Einrichtungen findet sich ein ähnliches Schema. Insbesondere kleinere Staaten wie die Dominikanische Republik und Palau

meldeten Datendiebstähle bei Ministerien. Daneben verzeichnet wurden zwei Datendiebstähle beim israelischen Verteidigungs- sowie dem Justizministerium, die mutmaßlich hacktivistisch motiviert sind und in Verbindung zum Vorgehen Israels im Gazastreifen stehen.

Angreiferprofile und Attributionen

Der April weist mit 49% einen leicht gesunkenen Anteil an komplett unattribuierten Cybervorfällen im Vergleich zum Vormonat März (54%) auf. Der Anteil an Operationen, der zwar hinsichtlich des Angreifertyps, nicht aber bezüglich des Ursprungslands näher benannt wurde, blieb mit 24% nahezu konstant (März: 25%). Die Liste der verzeichneten Ursprungsländer der im April zur EuRepoC-Datenbank hinzugefügten Cybervorfälle hat sich dagegen im Vergleich zum Februar mehr als verdoppelt: wurden im März lediglich Russland, China, Nordkorea, Iran sowie die Ukraine verzeichnet, umfasst die Liste für April elf verschiedene Länder, darunter auch die USA, Großbritannien und Polen. Hierfür zeichnete sich ein gemeinsamer Vorfall verantwortlich: So wurde Anfang April bekannt, dass die pro-ukrainische Hackergruppe OneFist im Januar dieses Jahres 100 GB an Daten des russischen Rüstungsunternehmens Special Technological Center LLC (STC) gestohlen habe. Zwar hatte das ukrainische Verteidigungsministerium bereits im Januar darüber berichtet, dass ihnen diese Daten zugespielt wurden, jedoch wurde weder mitgeteilt, von wem noch durch welche Mittel die Daten des russischen Konzerns erlangt worden waren. Es hätte sich daher auch um einen Insider-Job und keinen Hack durch OneFist handeln können, weshalb der Fall erst im April zur EuRepoC-Datenbank hinzugefügt wurde. Speziell OneFist, die für sich reklamieren, Mitglieder in den besagten drei sowie weiteren fünf nicht näher benannten Ländern zu haben, verdeutlicht einmal mehr die politische, sowie vor allem völkerrechtliche Problematik um die Involvierung nichtstaatlicher Hacker im Kontext des russischen Kriegs gegen die Ukraine. So hat die Ukraine seit Beginn der Kampfhandlungen im Februar 2022 nicht nur selbst eigenständige Hacktivisten-Gruppen, wie die IT Army of Ukraine, mit aufgebaut und seither mutmaßlich auch mit angeleitet, sondern der Gruppe OneFist nun sogar eine Art Auszeichnung für ihre Operationen gegen Russland verliehen. Übersetzt erhielten die Mitglieder, wie etwa der US-Amerikaner Kristopher Kortright (alias “Voltage”), Urkunden für „einen bedeutenden Beitrag zur Entwicklung und Aufrechterhaltung lebenswichtiger Aktivitäten des Militärs“. Hierdurch werden nicht nur einheimische Zivilisten, sondern sogar ausländische Staatsbürger direkt für Handlungen im militärischen Kontext belobigt, was sie aus völkerrechtlicher Sicht eben auch potenziell zu legitimen Zielen militärischer Gegenschläge durch Russland machen könnte. Hinzu kommt bei solchen Hacktivisten-Operationen stets das nicht zu kalkulierende Risiko ungewollter Schäden, bzw. von außer Kontrolle geratenen Operationen, die so nicht im Sinne der Ukraine (oder anderer demokratischer Länder) verlaufen sind. Auch hinsichtlich eines Nachkriegs-Szenarios stellt sich durchaus die Frage, was Menschen wie Kristopher Kortright tun werden, wenn sie ihre Zeit und Energie nicht mehr für das Hacken russischer Ziele aufwenden können. Zumal er nach eigenen Angaben seinen Job aufgrund seiner Hacking-Tätigkeiten verloren habe.



Zweimal im April vertreten waren Vorfälle, die belarussischen Angreifern zugesprochen wurden. In beiden Fällen handelte es sich um Hacktivisten-Operationen der Cyber-Partisans, die sich allerdings laut einem Washington Post Artikel aus im Ausland lebenden, belarussischen IT-Professionellen zusammensetzt. Neben dem bereits beschriebenen Fall gegen die Chemieanlage Hrodna Azot gab die Gruppe Ende April an, bereits im Herbst 2023 die Netzwerke des belarussischen Geheimdiensts KGB kompromittiert und unter anderem die Personalakten von über 8000 aktuellen und ehemaligen Mitarbeitern erbeutet zu haben. Auch wenn sich die Gruppe bereits vor der russischen Invasion im Februar 2024 durch Hacking-Operationen gegen das belarussische Schienennetz pro-ukrainisch zeigte, richten sich ihre Operationen im Kern gegen Lukaschenko. Dass sie in der Vergangenheit bereits für das Regime kompromittierende Daten gestohlen hatten, könnte in der Zukunft womöglich noch relevant werden, etwa im fiktiven Falle einer Anklage des Machthabers durch den internationalen Strafgerichtshof. Auch hierauf reagieren autokratische Regime jedoch bereits, ebenfalls mithilfe von Cyberoperationen, wie berichtete russische Hackingoperationen, mit dem Ziel, Beweismaterial zu möglichen Kriegsverbrechen in der Ukraine zu löschen oder zu erbeuten, verdeutlichen.

Im April konnten 17 Cyberoperationen konventionellen Konflikten zugeordnet werden. Mit sieben unterschiedlichen Konfliktdyaden ist dabei im Vergleich zu den meisten Vormonaten eine weitaus größere Diversität gegeben. Bislang hatten vor allem der Krieg zwischen Russland und der Ukraine, sowie ab Oktober 2023 die Dyade Israel - Hamas das Geschehen bestimmt. Im April wurden jedoch auch Cyberoperationen im Kontext weiterer, oftmals bereits sehr lange bestehender Auseinandersetzungen, mit jedoch nicht immer bereits gewaltsamen Austragungsmodus, verzeichnet: Belarus vs. Opposition; EU, USA et al. vs. Russland; Nordkorea vs. Südkorea; Iran vs. Israel; China vs. USA. Zahlenmäßig dominierte nach wie vor Russlands Krieg gegen die Ukraine auch den Cyberkonfliktaustrag im April, mit sieben verzeichneten Vorfällen, gefolgt von drei Operationen im Kontext des koreanischen Konflikts. Auch Israel vs. Hamas wurde dreimal verzeichnet.

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 Wissenschaftlerin 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).