European
Repository of
Cyber Incidents

EuRepoC

Cyber Conflict Briefing

Mai 2024

Jakob Bund
Kerstin Zettl-Schabath
Martin Müller

Beobachtungen zur Gesamtlage

Im **Mai 2024** wurden 73 Cyber-Operationen in die EuRepoC-Datenbank aufgenommen. Das sind 21,5% weniger als im Vormonat und 4 Operationen mehr als die insgesamt durchschnittlich verzeichnete Aktivität von 69 Cyber-Operationen pro Monat im Gesamtzeitraum.

Die **durchschnittliche Intensität** der im Mai 2024 erfassten Operationen beträgt 2,92 und liegt somit über dem historischen Durchschnitt (2,83). 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.

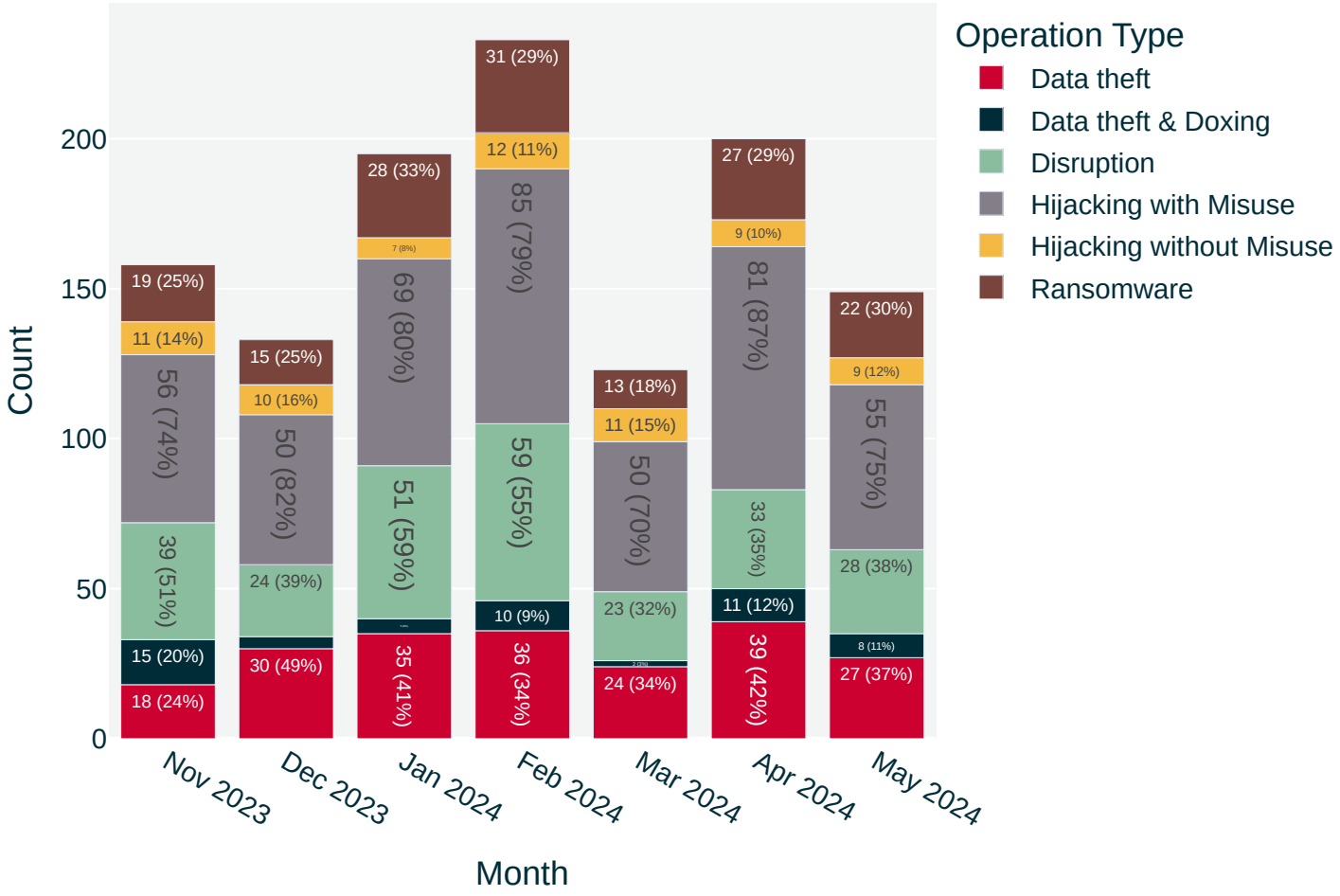
Über EuRepoC

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 Mai 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 56 Fällen (77%). Als Sammelbegriff fasst dies Aktionen, bei denen es Angreifern gelungen ist, in Systeme und Netzwerke einzudringen, um dort bereits unbefugt üblicherweise schädliche Aktionen auszuführen. Diese Aktivitäten werden, sofern erkennbar, weiter nach ihrer Absicht differenziert und können Datendiebstahl oder Betriebsstörungen umfassen.

Auf niedrigschwelliger Ebene können sich solche Operationen auch gegen einzelne Nutzerkonten richten. Am 10. Mai etwa erlangten Unbekannte Zugriff auf den X-Account der französischen Sportministerin Amélie Oudéa-Castéra, deren Ressort für die Ausrichtung der olympischen Sommerfestspiele verantwortlich ist, die am 26. Juli in Paris eröffnet werden.

Im vorliegenden Fall nutzten die Eindringlinge den Zugang, um Phishing-Nachrichten an andere Nutzer:innen der Plattform zu verschicken. Gerade in Hinblick auf Massenereignisse wie die olympischen Spiele stellen Social-Media-Accounts mit hoher Reichweite oder offizieller Autorität wie die von Politikern und Politikerinnen auch ein attraktives Ziel für Manipulationsversuche dar, insbesondere für Tätergruppen, mit der Absicht öffentliche Unsicherheit zu schüren.

Nachrichten über eine fingierte Notfallsituation lassen sich durch übernommene Accounts mit geringem Aufwand zumindest kurzzeitig schnell verbreiten, wenn sie gezielt über für ihr Sendungsvermögen ausgewählte Kanäle gestreut werden. Auch wenn sich solche Beeinflussungsversuche rasch aufklären lassen, sind diese in Echtzeit schwer in ihrer momentanen Wirkung einzudämmen, wenn das Ziel darin besteht, eine vorübergehende Panik auszulösen, Sicherheitsbehörden oder die gastgebende Regierung bloßzustellen und ein öffentliches Gefühl der Unsicherheit vor dem Hintergrund ernstzunehmender Sabotagedrohungen zu verstärken.

Russland hat in der Vergangenheit wiederholt Versuche unternommen, unter falscher Flagge terroristische Bedrohungen zu inszenieren. 2015 unterbrach die Gruppierung APT28 die Übertragung des französischen Fernsehsenders TV5Monde und veröffentlichte auf den Social-Media-Kanälen des Senders islamistische Propaganda. Dabei gab sich der dem russischen Militärgeheimdienst GRU zugerechnete Bedrohungsakteur unter dem Namen „Cyber Caliphate“ als eine dem Islamischen Staat nahestehende Verbindung aus. 2018 wandte sich die ebenfalls mutmaßlich durch eine GRU-Einheit gesteuerte Gruppe Sandworm bereits gegen die olympischen Winterspiele in Südkorea, in der Absicht, die Eröffnungsfeier durch einen Wiper-Angriff zu stören.

Der zweithäufigste im Mai 2024 festgestellte Operationstyp war 'Disruption'-Operationen (38%). Darunter verstehen sich Operationen mit dem Ziel, einen informationstechnischen Dienst außer Betrieb zu setzen. Eine Disruption oder Störung beeinträchtigt entsprechend dessen Verfügbarkeit. Störaktionen sind in aller Regel von vorübergehender Wirkung. Im Fall von Ransomware kann der blockierte Zugriff auf betriebswichtige Daten allerdings auch über einen längeren Zeitraum für Ausfälle sorgen. Von diesen Operationstypen sind für Mai 28 durch das Repositorium erfasst.
Unter Einsatz vergleichsweise wenig anspruchsvoller DDoS-Werkzeuge gelang es dem ukrainischen Militärnachrichtendienst HUR am 3. Mai, die Übertragung von Telekommunikationsanbietern in Tatarstan, einer der bevölkerungsreichsten autonomen Republiken im Osten Russlands, auszusetzen. Die zeitweisen Netzausfälle betrafen die Anbieter MTS, TATTelecom sowie den regionalen Betreiber Ufanet und konzentrierten sich auf die Wirtschaftszone Alabuga, in der sich über 30 Einrichtungen befinden, darunter mehrere kritische Unternehmen der Verteidigungsindustrie.

Auch primitive Aktionen wie DDoS-Angriffe können dazu geeignet sein, in einer unübersichtlichen Lage den Informationsfluss kurzfristig einzuschränken oder Kommunikation zu behindern, auch wenn sie üblicherweise leicht zu entschärfen sind.

Im Rahmen einer Großveranstaltung und in Verbindung mit zeitlich abgestimmten Versuchen, bewusste Falschmeldungen über einen Notfall in Umlauf zu bringen, könnten DDoS-Angriffe gegen zentrale Nachrichtenportale oder Regierungsstellen zu Verunsicherung beitragen. In einem vergleichbaren Szenario waren im März die Webseiten von Behörden und Ministerien nach einem DDoS-Angriff der selbsternannten Hacktivistengruppe Anonymous Sudan auf die französische interministerielle Behörde für Digitales (DINUM), die für die Verwaltung von mehr als 300 Regierungsdomains verantwortlich ist, über mehrere Stunden nicht erreichbar.

Die Kombination von DDoS-Angriffen und Social-Media-Account-Übernahmen können dabei ein absichtlich einfach gehaltenes Toolkit darstellen, das grundsätzlich glaubhaft von Hacktivisten einzusetzen ist. Etwaige staatliche Auftraggeber könnten diese Ausgangslage nutzen, um ihre Verantwortung zu verdecken oder zumindest für ausgewählte Zielgruppen abzustreiten. Der potentielle Effekt liegt dabei weniger in den Operationen selbst, sondern in deren psychologischen Wirkung.

DDoS-Kampagnen hacktivistischer Formierungen mit vermuteten Verbindungen nach Russland, wie Anonymous Sudan, NoName057(16) oder KillNet, zeugen von anhaltenden Bemühungen, die geringfügigen Beeinträchtigungen dieser Aktionen heraufzuspielen.

Brennpunkte und Zielmuster

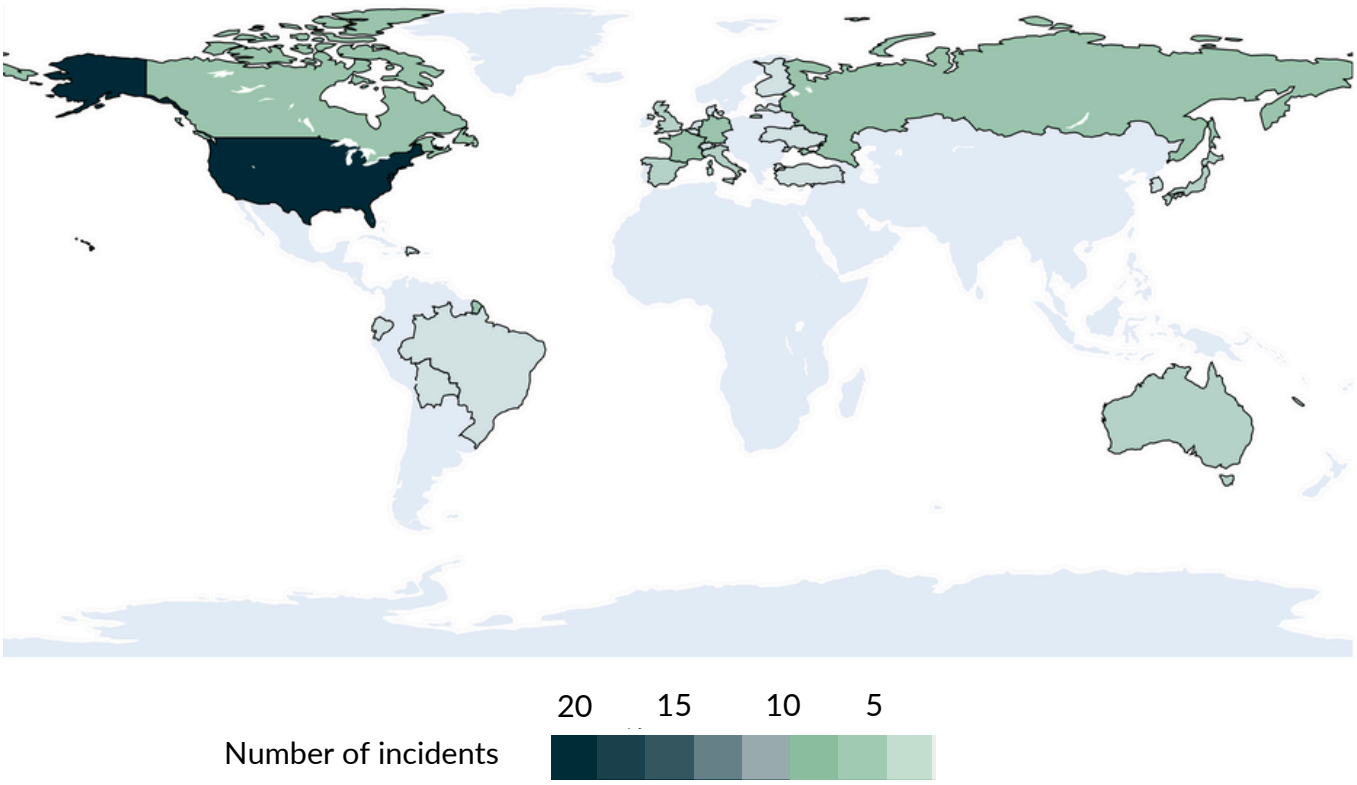
Der am häufigsten im Mai 2024 betroffene Zielsektor waren Unternehmen der kritischen Infrastruktur mit 44 neu aufgenommenen Fällen, was in relativen Zahlen 60% entspricht. Am zweithäufigsten betroffen waren in 26 beziehungsweise 36% der Fälle staatliche Institutionen. In beiden Bereichen handelt es sich im Vergleich zum April damit um einen Rückgang von 17% bei kritischen Infrastrukturen, bei staatlichen Institutionen sogar um 38%.

Recht hoch ist weiterhin die Zahl der aufgenommenen Vorfälle für sonstige Unternehmen, die nicht Teil der kritischen Infrastruktur sind: Anhand der Inklusionskriterien von EuRepoC werden solche Vorfälle nicht grundsätzlich berücksichtigt. In zwei Ausnahmen werden allerdings auch Unternehmen außerhalb der kritischen Infrastruktur in die Datenbank aufgenommen. Dies kann zum einen sein, wenn eine „Politisierung" stattgefunden hat, also ein Angriff einem politischen Akteur zugeschrieben werden kann oder Teil der öffentlichen Debatte geworden ist. Zum anderen ist dies der Fall, wenn das Unternehmen zusätzliches Ziel ist, also etwa neben einem Unternehmen der kritischen Infrastruktur auch betroffen ist. Dies war im Mai in sechs Vorfällen der Fall.

Unter den Staaten am häufigsten betroffen waren wie in Beobachtungen für vorangegangene Monate die Vereinigten Staaten, dieses Mal in 20 Fällen. Mit 19 Fällen waren die Mitgliedsstaaten der EU annähernd gleich oft betroffen. Frankreich war hier mit fünf Vorfällen vertreten, gefolgt von Deutschland mit vier und Italien mit drei.

Bei einem Blick auf die betroffenen Sektoren kritischer Infrastruktur wurden mit neun die meisten Fälle erneut für den Gesundheitssektor aufgenommen. Zwar sind nur für zwei der Fälle Ransomwaregruppen als mutmaßliche Urheber bekannt geworden, doch sprechen mehrere Faktoren dafür, dass weitere kriminelle Akteure hinter den verbleibenden Vorfällen stecken: Geografisch lässt sich zunächst ein Schwerpunkt in Nordamerika erkennen, der sich mit bisherigen Beobachtungen deckt. Weiterhin wurde in fast allen Vorfällen ein Datendiebstahl registriert, der zudem von den betroffenen Organisationen selbst bekannt gegeben und dann in der breiten Medienberichterstattung aufgegriffen wurde, statt etwa durch technische Berichte von IT-Sicherheitsunternehmen. Eine Ausnahme hiervon stellt der Vorfall beim Rezeptdienstleister MediSecure in Australien dar, der zunächst durch die dortigen Cybersicherheitsbehörden mitgeteilt wurde. Angesichts des erheblichen Umfangs an betroffenen Daten mit kolportierten 6 Terabyte erinnert der

Geographic distribution of operations



Vorfall an jenen bei der Krankenversicherung Medibank im Oktober 2022. Zu Beginn dieses Jahres hatten Australien, Großbritannien und die Vereinigten Staaten gegen einen der mutmaßlichen Urheber mit gemeinsamen Sanktionen reagiert.

Mit sieben Vorfällen waren der Energiesektor und Bereich kritische Fertigung am zweithäufigsten von den Sektoren der kritischen Infrastruktur betroffen. Für den Energiebereich lässt sich als eine Bedrohung wie auch in anderen Sektoren Ransomware ausmachen. Für den Mai lässt sich exemplarisch aber auch eine zunehmende Bedrohung durch selbst-erklärte russische Hacktivisten ausmachen, die mutmaßlich als Tarnung für russische Geheimdienste agierten. So berichteten mehrere US-amerikanische Behörden von Versuchen dieser Akteure, kleinere Wasserversorger, aber auch andere Bereiche kritischer Infrastruktur über online erreichbare Kontrollsysteme für disruptive Zwecke zu kompromittieren.

Ransomware bleibt auch für den Bereich der kritischen Fertigung eine Bedrohung, wie es die Fälle bei dem US-amerikanischen Optikproduzenten Omnivision oder Nissan Nordamerika zeigen. Wie im letzten Monat schon am Beispiel Volkswagen beschrieben, sind es in diesem Sektor insbesondere auch Fälle von Industriespionage, die ein spezifisches Risiko darstellen. Ein Beispiel hierfür lässt sich durch die Nordkorea zugerechnete Gruppierung Moonstone Sleet finden, welche seit Dezember 2023 mehrere Unternehmen im Luftfahrtsektor zum Ziel hatte, unter anderem um Know-how zu erlangen.

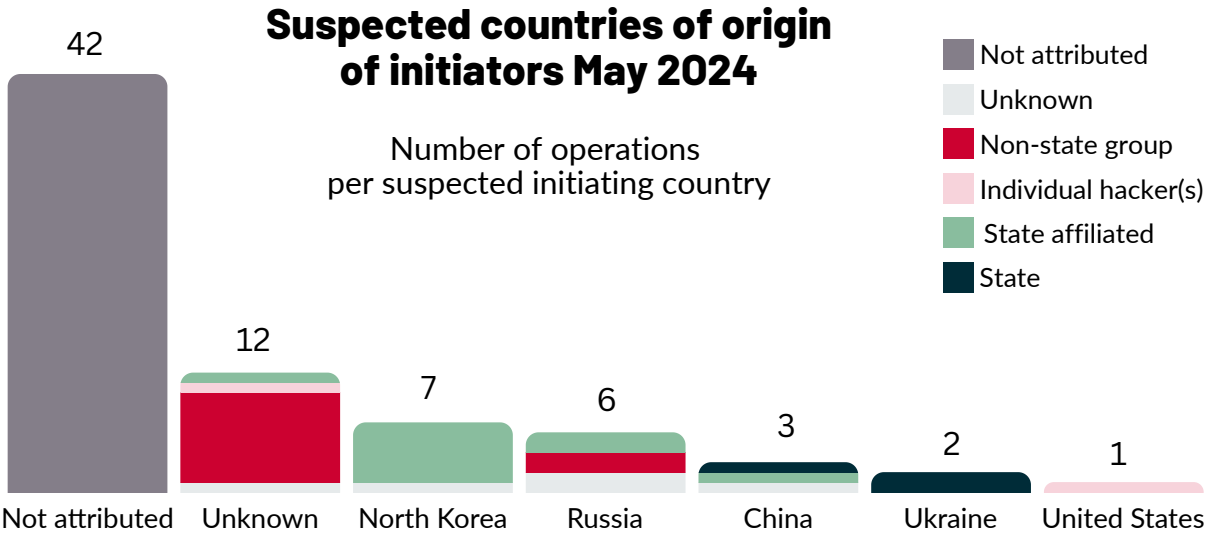
Bei staatlichen Institutionen zeigt sich mit 16 Fällen erneut eine höhere Betroffenheit nachrangiger Verwaltungseinheiten, in Deutschland etwa ein Ransomwareangriff auf die Hessische Hochschule für öffentliches Management und Sicherheit. Auf höherer Verwaltungsebene wurden für den Mai neun Vorfälle aufgenommen. Das auch hier durchaus schwerwiegende Vorfälle ereignen können, zeigt etwa der

Angriff auf Shared Services Connected, einem Dienstleister der englischen Sicherheits- und Verteidigungsbehörden, bei dem Daten zur Gehaltsabrechnung der britischen Streitkräfte abflossen oder der erst jetzt bekannt gewordene Datendiebstahl bei einem unbenannten europäischen Außenministerium durch russische Akteure.

Angreiferprofile und Attributionen

Der Mai weist mit 58% einen um 9% gestiegenen Anteil an komplett unattribuierten Cybervorfällen im Vergleich zum Vormonat April (49%) auf. Der Anteil an Operationen, der zwar hinsichtlich des Angreifertyps, nicht aber bezüglich des Ursprungslands näher benannt wurde, sank von 24% im April auf nun 15%. Die Liste der verzeichneten Ursprungsländer der im Mai zur EuRepoC-Datenbank hinzugefügten Cybervorfälle hat sich dagegen im Vergleich zum April wieder stark reduziert und umfasst außer dem Iran die am häufigsten attribuierten Autokratien, aber auch die Ukraine sowie die USA. Für letztere ist ein Fall mit mutmaßlich rein persönlicher Motivation verantwortlich: So soll ein Student aus Texas angeblich seinen Schul-Laptop benutzt haben, um Distributed Denial of Service (DDoS)-Angriffe zu initiieren, wodurch die Internetdienste während der staatlich vorgeschriebenen Tests (STAAR) im Bezirk gestört wurden. Dies betraf alle Schulen und beeinträchtigte etwa 3.000 Schüler, die ihre Tests unterbrechen und neu starten mussten. Am nächsten Tag wurden 700 Schüler von den Tests ausgeschlossen und mussten aufgrund der Störungen ihre STAAR-Tests wiederholen. Der Fall verdeutlicht zweierlei: erstens, wie leicht es für Personen mit wenig sophistizierten technischen Fähigkeiten geworden ist, ihre Ziele mit Hilfe von Cybertools zu verfolgen, etwa DDoS-Operationen. Dieser Trend wird sich vermutlich durch immer leichter zugängliche KI-Anwendungen zudem noch verstärken und auch komplexere Operationen für solche Personenkreise ermöglichen. Zweitens, dass Cyberoperationen nicht ausschließlich durch böswillige ausländische Täter:innen erfolgen, sondern ebenfalls auch Insider Systeme stören und Schaden verursachen. Ein jüngeres Beispiel hierfür ist ein Fall aus Singapur: Verärgert über seine Entlassung griff ein Mann auf die Computersysteme seines ehemaligen Unternehmens zu und löschte 180 virtuelle Server, was einen Schaden von S$918.000 (US$678.000) verursachte. Am 10. Juni wurde er wegen unbefugten Zugriffs auf Computermaterial zu zwei Jahren und acht Monaten Haft verurteilt. Ein umfassendes Account Management wird als Cybersicherheitsmaßnahme oftmals unterschätzt, sollte aber gerade im Hinblick auf solche Szenarien im Rahmen von Cybersicherheitsstrategien stärkere Beachtung finden.

Auf Seiten der attribuierten direkt-staatlichen Angreifer setzte die Ukraine auch im Monat Mai ihre offensive Kommunikationsstrategie eigener Operationen gegen russische Ziele fort. So störte der HUR ab dem 7. Mai 2024 den russischen Softwareentwickler 1C und den Cloud-Anbieter Cloud4y, nachdem sich der HUR wie eingangs beschrieben ebenfalls für einen Internetausfall in Tatarstan am 3. Mai mit Hilfe einer DDoS-Operation verantwortlich gezeichnet hatte. In beiden Fällen wurden die Operationen auf indirektem Wege „selbstattribuiert“, durch anonym bleibende Geheimdienstquellen. Ein Grund für dieses „Durchstechen“ an Medien könnte sein, dass die eigene Operation zwar publik gemacht werden sollte, gegenüber der eigenen, aber auch der russischen Bevölkerung, jedoch beide Ziele, das



Software-Unternehmen, als auch die Telekommunikationsanbieter, ziviler Natur und daher aus völkerrechtlicher Sicht eigentlich keine legitimen Ziele von schadhaften Operationen im Kontext militärischer Auseinandersetzungen sind.

Laut Sicht des Auswärtigen Amts und internationaler Organisationen wie dem Internationalen Komitee vom Roten Kreuz, wären Militäroperationen gegen zivile Ziele nur dann legitim, sofern nachweisbar wäre, dass die angegriffenen Systeme direkt für militärische Zwecke verwendet worden sind. Ferner stehen kritische Infrastrukturen, zu denen auch Telekommunikationsanbieter gehören, unter besonderem Schutz, wie es etwa auch im Rahmen der UN Normen zu verantwortungsvollem Staatenverhalten im Cyberspace für Friedenszeiten verankert ist. Natürlich attackieren russische Akteure ebenfalls in starkem Maße kritische Infrastrukturen und zivile Ziele, neben Operationen im Cyberspace zumeist mit sehr viel schwerwiegenderen Folgen auf konventioneller Ebene. Dennoch zeigt das Vorgehen der Ukraine, dass gerade demokratisch geprägte Staaten bei der Nutzung von Cyberoperationen im militärischen Kontext oftmals noch komplexe Kosten-Nutzen-Abwägungen zu treffen haben, auch hinsichtlich der Kommunikation der eigenen Operationen.

Auf Seiten der prävalenten konventionellen Konflikte dominierte auch im Mai einmal mehr der Krieg zwischen Russland und der Ukraine, mit sieben verzeichneten Vorfällen. Desweiteren wurden zwei Konfliktdyaden mit jeweils einer zugeordneten Cyberoperation aufgenommen, nämlich Nordkorea-Südkorea und Vietnam/et al.-China im Kontext der Streitigkeiten um das Südchinesische Meer. Letzterer Fall ist aus mehreren Gesichtspunkten heraus interessant: Zum einen machte Bitdefender für die entdeckte, mehrjährige Spionageoperation gegen acht militärische sowie staatliche Ziele in der Region des Südchinesischen Meeres eine vorher noch nicht entdeckte APT verantwortlich, der das Unternehmen den Namen „Unfading Sea Haze“ gab. Deren Aktivitäten entsprechen laut Bitdefender chinesischen Interessen im Rahmen des Territorial- und Ressourcenkonflikts, was zusätzlich zu weiteren Übereinstimmungen mit chinesischen APT-Mustern eine zumindest vorläufige Attribution in Richtung China plausibel erscheinen lässt.

Des Weiteren handelt es sich bei Unfading Sea Haze mutmaßlich um keine neue Formierung, sondern eine staatlich-gesponserte Gruppe, der es gelungen ist, über fünf Jahre unentdeckt zu bleiben. Ferner kompromittierte sie Systeme nicht nur einmal, sondern verschaffte sich immer wieder Zugang zu diesen, was einmal mehr die Folgen mangelnder Hygiene beim Verwalten von Zugangsdaten sowie unzureichender Patching-Praktiken auf exponierten Geräten und Webdiensten verdeutlicht. Der mutmaßliche Fall chinesischer Cyberspionage im Kontext des Konflikts reiht sich ein in eine Vielzahl ähnlicher Kampagnen, nicht nur gegen Ziele in Vietnam (aktuell 18 verzeichnete Fälle in der EuRepoC-Datenbank seit 2005), sondern auch gegen die Philippinen (19 erfasste Operationen, ebenfalls seit 2005) oder Malaysia (11 erfasste Operationen, seit 2011). Die noch weitaus zahlreicheren chinesischen Spionageoperationen gegen taiwanesische Ziele lassen sich dagegen oftmals nicht eindeutig dem bilateralen Konflikt zwischen China und Taiwan um die Sezessionsbestrebungen der Insel einerseits, oder dem Regionalkonflikt andererseits zuordnen. Die beschriebenen Aktivitäten demonstrieren die strategische Instrumentalisierung von Cyberoperationen chinesischer APTs im Rahmen zahlreicher nationaler, sowie regionaler Konflikte. Die dabei unter Chinas Präsident Xi Jinping immer stärker voran getriebene Integration von Cyberfähigkeiten in übergeordnete Militärstrategien verdeutlicht jedoch, dass es dabei in Zukunft auch von chinesischer Seite zu noch stärker disruptiven Cyberoperationen, etwa gegen militärische, aber auch kritische Infrastrukturen kommen könnte. Wer hierfür im innerchinesischen Machtgefüge hauptverantwortlich sein wird, der technologische Arm der Volksbefreiungsarmee (PLA) oder zumindest auch in Teilen das Ministry of State Security, wird sich noch zeigen müssen, speziell nach der im April bekannt gewordenen Auflösung der erst 2015 gegründeten Strategic Support Force der PLA, die für genau dieses Operationsprofil bislang verantwortlich war und nun in drei Bereiche aufgeteilt wurde (Aerospace, Cyber, Information Support Forces).

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.