Internationale Cyberkonflikte: Der Blick auf Deutschland und die Welt

Kerstin Zettl-Schabath & Sebastian Harnisch, Universität Heidelberg

IFSH-Workshop, Auswärtiges Amt Berlin, 23. Juni 2022

In ihren Lageberichten zur Cybersicherheit in Deutschland zeichnen das Bundesministerium des Innern (BMI 2021: 12) und das Bundesamt für die Sicherheit (BSI 2021) in der Informationstechnologie ein dynamisches Lagebild: die Vergrößerung des deutschen Angriffsvektors, der durch die stetige Digitalisierung weiterer Lebens- und Wirtschaftsbereiche und zuletzt die Home-Office-Regelungen vieler Betriebe wächst; die Zunahme von Ransomware-Attacken mit immer sophistizierterer Schadsoftware; sowie die Wirkung von Sondereffekten wie der Corona-Pandemie, welche insbesondere den Gesundheitssektor in den Mittelpunkt cyberkrimineller Aktivitäten rückte (BMI 2021; BSI 2021). Wir ergänzen dieses Lagebild durch den Blick auf internationale Cyberkonflikte und die Risikolage für die Bundesrepublik.

Eine Grundlage dieses internationalen Lagebildes ist der Heidelberger Datensatz HD-CY.CON 1.0, der weltweit politisierte Cyberangriffe seit 2000 verzeichnet und bis zum Operationsstartjahr 2021 mehr als 1.500 Ereignisse anhand technischer und politischer Kategorien kodiert hat (https://doi.org/10.11588/data/KDSFRB).[i] In diesem Datensatz werden Angriffe erfasst, welche die technischen Inklusionskriterien, die Kompromittierung der Confidentiality (Vertraulichkeit), Integrity (Integrität) und Availability (Verfügbarkeit) sowie die politischen Inklusionskriterien 1) Politische/staatliche Akteure als Angreifer; 2) Politische/staatliche Akteure als Opfer und 3) Politisierung des Vorfalls, z.B. Cyberkriminalität, umfasst.

Der Blick auf die Varianz der angreifenden Akteure ergibt folgendes globales Lagebild: das Spektrum von staatlichen und nichtstaatlichen Angreifern wird über Zeit, insbesondere nach 2010 deutlich breiter; realpolitische Ereignisse, bspw. der Arabische Frühling, aber auch formative „Cyber-Ereignisse“ wie das Bekanntwerden von Stuxnet, können katalytische Wirkung für bestimmte Gruppen haben; (nichtstaatliche) Hacktivisten verüben das Gros der verzeichneten Angriffe, ihre Angriffe entfalten aber weniger Schadwirkung als jene staatlicher oder staatlich-gestützter Angreifer (Grafik 1). Unter den Angriffstypen (Sabotage, Spionage und Kriminalität) nehmen cyberkriminelle Angriffe, insbesondere Ransomwarevorfälle, den größten Teil ein, die seit Mitte der 2010er Jahre stärker politisiert und in der Abfolge durch innerstaatliche strafrechtliche Instrumente bekämpft werden (Grafik 2).[ii]

Unter den (in HD-CY.CON verzeichneten) angreifenden Akteuren stechen jene aus vier autokratischen Staaten hervor, der VR China, der Russischen Föderation, der Islamischen Republik Iran und der Demokratischen Volksrepublik Korea (mehr als 90% aller autokratischen Angriffe). Wichtig ist, dass die überwiegende Mehrzahl dieser Angriffe von sog. „Cyber-Proxys” verübt wurde, wobei deren Anbindung an staatliche Stellen über Zeit und die Verwendung von Schadsoftware stark variieren kann. (Grafik 2). Zusätzlich lässt sich in jüngster Zeit eine wachsende Diversifizierung der Hacking-for-Hire-Lieferketten in der Proxy-Nutzung beobachten: Ein russischer Oligarch engagiert einen israelischen Privatdetektiv, der wiederum indische Cyberkriminelle damit betraut, im Auftrag des Oligarchen Cyberspionage zu betreiben; ein Kardiologe aus Venezuela bringt sich das Programmieren bei und verkauft Software an iranische Hacker, die diese gegen israelische Firmen einsetzen (Grafik 3).

Der Blick auf Deutschland als Angriffsvektor zeigt Folgendes: Die in HD-CY.CON erfassten Angriffsakteure und ihre Ziele spiegeln die temporäre Verteilung auch auf globaler Ebene wider; als gewichtiger Industriestandort sind deutsche Unternehmen und Forschungseinrichtungen ein logisches und wiederkehrendes Ziel chinesischer Akteure; das Verlaufsmuster russischer Hack-and-Leak-Operationen[iii] und politischer Spionageoperationen entspricht weitestgehend dem generellem Anstieg solcher russischen Operationen in Folge des Ukrainekriegs

ab 2014; mit wenigen Ausnahmen hatten russische Angriffe bislang keine disruptive Wirkung auf deutsche Ziele. Seit 2017 lassen sich auch die charakteristisch opportunistischen nordkoreanischen Cyberangriffe in Deutschland nachweisen: Sie zielen primär auf die Generierung finanzieller Ressourcen für das Regime und seine (atomare) Aufrüstungspolitik sowie Industriespionage, um seine ballistischen Raketenprogramme (schneller) weiterentwickeln zu können (Grafik 4).

Lassen Sie uns noch einen Blick auf die Auswirkungen des Ukrainekrieges und das Lagebild in Europa und Deutschland werfen. Mischa Hansel wird noch vertieft auf den Ukrainekrieg im Cyberraum eingehen. Deshalb hier der Blick auf die Frage, inwiefern Lieferungen konventioneller Waffen an die Ukraine einen Effekt auf die Zielsetzung von russischen Cyberangriffen gegen westliche Staaten haben?

Grafik 5 zeigt auf der linken Seite eine Rangliste von Waffenlieferländern hinsichtlich ihrer militärischen Unterstützung (in Mrd. Euro). Auf der rechten Seite ist eine Rangliste von Waffenlieferländern ausgewiesen, die zum Opfer von russischen Cyber-Operationen geworden sind. Die Gesamtanzahl der russischen Cyber-Operationen ist so dargestellt, dass sie die Cyber-Operationen nach der Ankündigung von Waffenlieferungen bzw. nach der erfolgten Waffenlieferung verzeichnet. Folgende tentative Interpretationen lassen sich plausibilisieren: 1) Es gibt Indizien dafür, dass die Ankündigung von Waffenlieferungen als auch deren Auslieferung einen verstärkenden Effekt auf russische Cyberangriffe hat; 2) da die meisten Waffenlieferländer auch sanktionierende Staaten gegen Russland sind und bereits vor der Invasion regelmäßig Ziel russischer Cyberakteure waren, lässt sich die kausale Wirkung von Waffenlieferungen nicht als statistisch signifikant ausweisen; bislang ist nur ein Fünftel der Angriffe (5 von 21 Ereignissen) auf militärisch-signifikante Ziele gerichtet; 3) die Anzahl der russischen Cyberangriffe vor und nach der Ankündigung bzw. Lieferung von Waffen ist aber vergleichsweise gering und diese Angriffe sind bislang wenig schwerwiegend, sodass eine abschreckende Wirkung auf zukünftige Waffenlieferungen nicht plausibel erscheint. Schließlich: Sofern die erfassten Angriffe die reale Situation widerspiegeln, werden Staaten wie Deutschland und Rumänien, die vergleichsweise weniger Waffen liefern, häufiger angegriffen, sodass deren technische und/oder politische Verletzlichkeit von russischen Akteuren (offensichtlich) als höher eingeschätzt werden als andere Staaten, die Waffen an die Ukraine liefern (Grafik 5).

Insgesamt sind Cyberspionageoperationen russischer Akteure mit staatlichem Hintergrund gegen waffenliefernde Länder auch in der Zukunft wahrscheinlicher als disruptive Cyberoperationen zur Abschreckung und/oder Bestrafung. Für Deutschland könnte dies, aufgrund des beschlossenen Sondervermögens der Bundeswehr, speziell den Rüstungssektor betreffen. Gleiches gilt für die Energiewirtschaft sowie für zivilgesellschaftliche Akteure und auch für geflüchtete ukrainische Oppositionelle und Cyber-AktivistInnen in europäischen Ländern.

Vorbehalt

Daten werden erst durch ihre regelgeleitete Interpretation zu (gesichertem) Wissen. Dies gilt insbesondere für Daten aus dem Cyberraum, deren Validität regelmäßig umstritten ist. Es sei daher ausdrücklich auf folgende Einschränkungen der verwendeten Daten und Datensätze hingewiesen: 1) Die Daten stammen nur aus öffentlich zugänglichen Quellen; 2) ein erheblicher Teil der Cybersicherheitsforschung geht zudem davon aus, dass sowohl Angreifende als auch angegriffene Akteure ein Interesse am beiderseitigen Verschweigen von Angriffshandlungen, u.a. zum Zweck der Eskalationskontrolle, haben. 3) Die in HD-CY.CON 1.0 und EuRepoC 1.0 erfassten Daten verzeichnen viele cyberkriminelle Operationen nicht, sondern lediglich jene, die zum Gegenstand politischer oder rechtlicher Handlungen wurden, bspw. Anklagen. 4) Die technische, politische und rechtliche Attribution von Cyberangriffen ist komplex und zeitaufwändig. Erkenntnisse über Schadprogramme und Vorgehensweisen, Schadwir-

kung und Akteurschaft etc. lassen sich zumeist erst über Zeit erhärten. Die Qualität von Attributionsprozessen lässt sich daher u.a. über die Transparenz der Kodierkriterien und die Dokumentation der Kontestation von Attributionsaussagen steigern.

Literatur und Quellenverzeichnis

BMI (2021): Cybersicherheitsstrategie für Deutschland 2021, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=1

BSI (2021): Die Lage der IT-Sicherheit in Deutschland 2021, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf?__blob=publicationFile&v=3

https://heidata.uni-heidelberg.de/dataset.xhtml?persistentId=doi:10.11588/data/KDSFRB

https://www.reuters.com/world/israeli-private-detective-used-indian-hackers-job-russian-oligarchs-court-filing-2022-05-27/

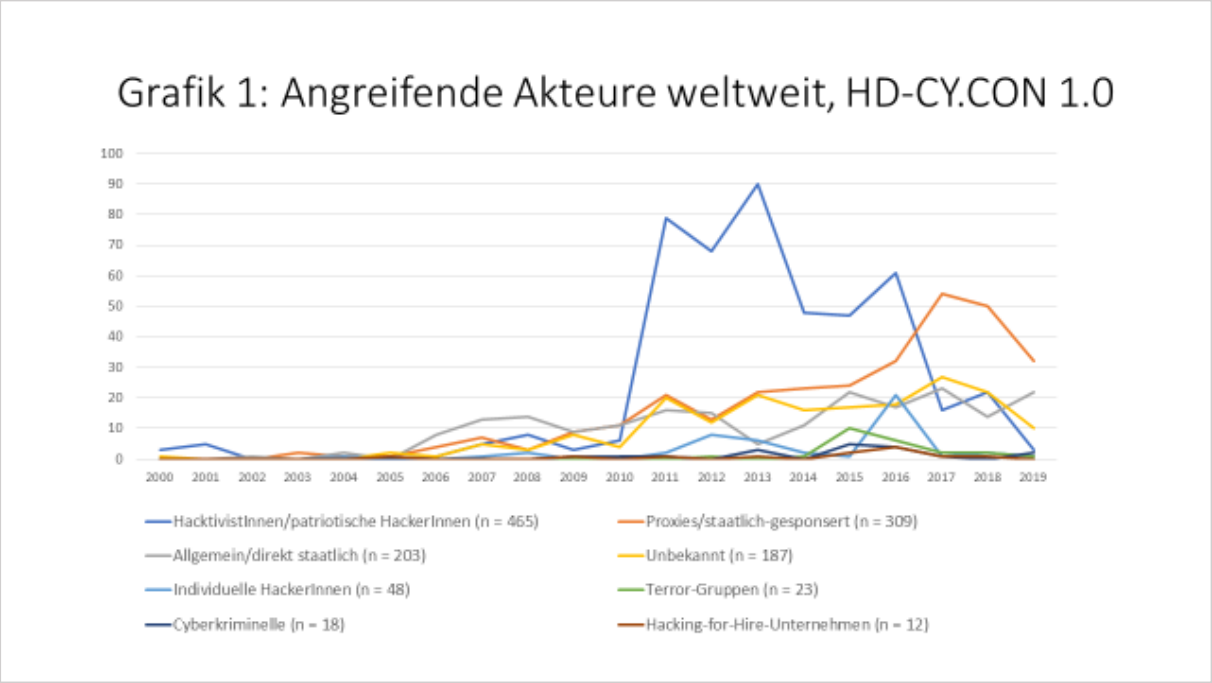
https://www.reuters.com/legal/government/us-charges-venezuelan-doctor-with-selling-ransomware-used-by-iranian-group-2022-05-16/

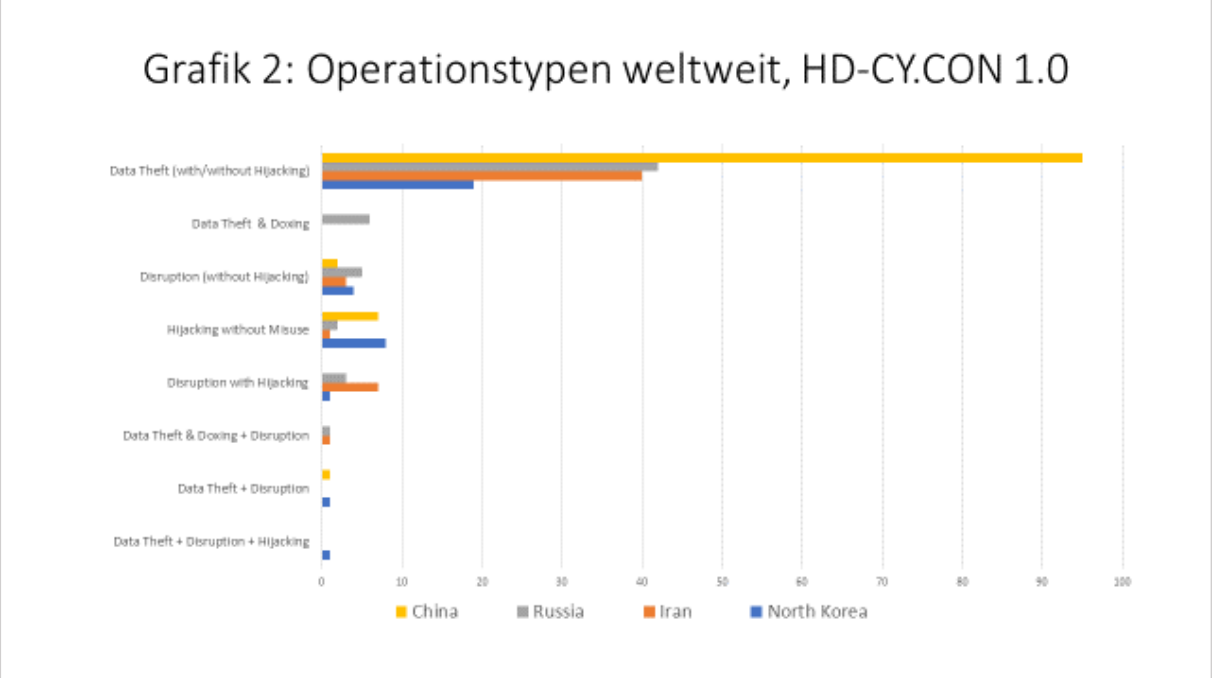
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

https://securityaffairs.co/wordpress/?s=newsletter

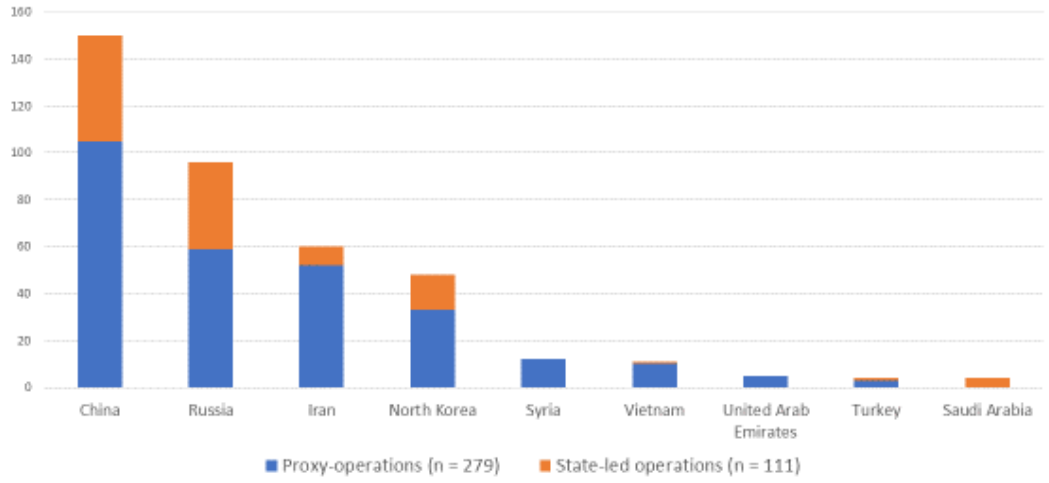
sowie Daten aus dem unveröffentlichten Datensatz EuRepoC 1.0

Anhang


Grafik 1: Angreifende Akteure weltweit, HD-CY.CON 1.0
100
90
80
70
60
50
40
30
20
10
0
2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019
HacktivistInnen/patriotische HackerInnen (n = 465)
Proxies/staatlich-gesponsert (n = 309)
Allgemein/direkt staatlich (n = 203)
Unbekannt (n = 187)
Individuelle HackerInnen (n = 48)
Terror-Gruppen (n = 23)
Cyberkriminelle (n = 18)
Hacking-for-Hire-Unternehmen (n = 12)


Grafik 2: Operationstypen weltweit, HD-CY.CON 1.0
Data Theft (with/without Hijacking)
Data Theft & Doxing
Disruption (without Hijacking)
Hijacking without Misuse
Disruption with Hijacking
Data Theft & Doxing + Disruption
Data Theft + Disruption
Data Theft + Disruption + Hijacking
0 10 20 30 40 50 60 70 80 90 100
China
Russia
Iran
North Korea

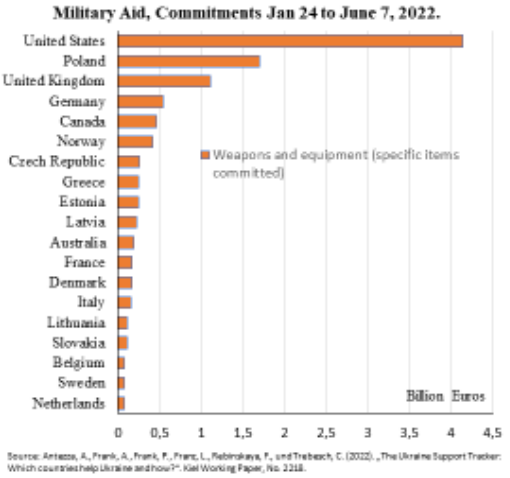
Grafik 3: Autokratische Cyberoperationen, HD-CY.CON 1.0

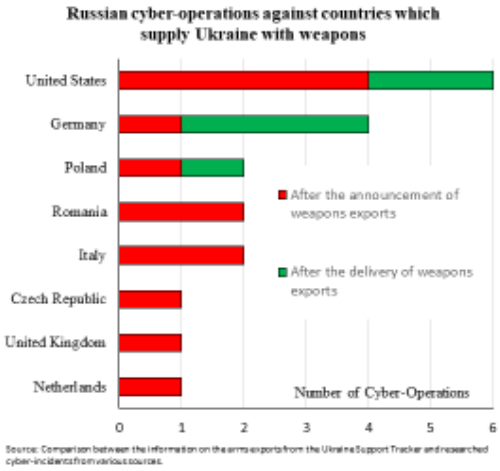


Grafik 4: Angreiferakteure gegen Ziele in Deutschland (HD-CY.CON)

	China	Russland	Iran	Nordkorea	Vietnam	Äthiopien	Frankreich	USA/Großbritannien	Hacktivisten
2006	APT1/Comment Crew; Stone Panda/APT10								
2007	Unknown Group								
2008								NSA/GCHQ	
2009	MSS						Snowglobe/ Babar		
2010	Turbine Panda/Hippo Team (MSS)								No-Name-Crew
2011	APT40/Leviathan (MSS)								No-Name-Crew; Anonymous
2012	Mofang		Magic Hound/APT35 Copy Kittens; Mabna Institute/ Silent Librarian						
2013									
2014	Stone Panda/APT10; APT3/Buckeye; Winnti Group				APT32/Ocean Lotus				Team System DZ
2015		APT28/Fancy Bear; Cyber Berkut							
2016			APT33			Staatlicher Akteur			
2017	APT20; MSS	Energetic Bear; Sandworm		Lazarus					
2018	Winnti Group			Lazarus					

Grafik 5: Russische Cyberangriffe gegen Staaten, die Waffen an die Ukraine liefern





---

i Der Datensatz HD-CY-CON 1.0 wird seit 2021 mit einem erweiterten Kategorienset (primär technische und rechtliche Indikatoren) als Datensatz EuRepoC 1.0 fortgeführt, der im September 2022 veröffentlicht wird.

ii Der Datensatz HD-CY-CON 1.0 verzeichnet diese Zunahme von Ransomewareangriffen noch nicht. EuRepoC 1.0 wird jedoch jene Ransomeangriffe erfassen, die ab dem 01.01.2022 politisch bedeutsam geworden sind.

iii Der HD-CY.CON erfasst keine reinen Desinformationskampagnen, wie z.B. Fake News auf Social Media Plattformen.